# EPING October 2007

*This is an archived edition of EPing, first published in October 2007. Although every effort has been made to preserve the original content, errors may have crept in and links may no longer be available.*

PING!
The HP User Group Technical Journal

## From The Chair -

I am handing this section over to someone else this time round as I am currently on leave and it is surely time for you to have the chance to hear from others on the hpUG Management Team. I am grateful to Ian Severn for stepping in to say a few words.

Well now, with the boss away in the desert in Colorado (no he has NOT deserted us!) here's an opportunity to have a quick review from the Admin and Events Team.

It is now one year since we moved out of DECpark in Reading to Amen Corner in Bracknell. Our fears of wondering how we could possibly manage to consolidate the whole of our filing from 3 cabinets and a "storage cage" into 3 drawers were actually un-founded as Angela and I have learned to be more ruthless about answering the question - "Do we REALLY need to keep this for 7 years?" This is not something that either of us is able to do in our own domestic situations! We have also learned the need to be more responsible for backing up the hpUG database and the accounts – something we took for granted in Reading.

We have continued to see the hpUG membership grow – our active list has increased to over 1570 (some 21% up on the same period last year). We have also seen that in recent weeks we have had an increase in the number of attendees at meetings, and over the year an increase in hpUG members taking up discounts on HP Education. Training Courses. So our financial position has definitely improved.

Equally important is that our working relationships with HP in the UK, EMEA and Corporate world is at an all-time high. I have also just returned from the European ITUG Conference in Brighton where we were able to share our thoughts with International representatives from the Encompass, ITUG and Vivit User Communities on how best we can serve all users of HP technologies throughout the world irrespective of our "heritage". There will be ways that hpUG members will benefit from these collaborations in the coming months.

You will already have received your invitation to tell us more about yourselves and your Companies so that we can better serve you in the future. Someone will be lucky and will win the Digital Camera and Printer – but in order to be eligible, please return the Survey to us or fill it in on–line by going to www.hpug.org.uk and pressing the "Survey" Button.

Ian Severn (General Manager of hpUG)

The theme for the October EPING is Networking and we hope you enjoy the issue. Please mail all comments (good or bad) to admin@hpug.org.uk

I look forward to hearing from you.

**John Owen**
*HPUG Chairman*
Take a look at our events page for the latest information on forthcoming events:
http://www.hpug.org.uk/index.php?option=com_events&Itemid=45

## Tips and Techniques from Bill Hassell

**For this issue, I have collected a number of favorite tips and techniques for writing scripts. In keeping with the Networking theme, here is a method to parse out the 4 octets in an IP address:**

```
MYADDR=10.23.45.67
echo $MYADDR | IFS=. read ADDR1 ADDR2 ADDR3 ADDR4
echo $ADDR1 $ADDR2 $ADDR3 $ADDR4
10 23 45 67
```

**To reduce fully qualified domain names such as cpu1.mysite.com to just cpu1:**

```
MYCPU=cpu1.mysite.com
echo ${MYCPU%%.*}
cpu1
```

**By using shell built-ins, the overhead in calling external routines can be eliminated.**

**Here are some shell constructs that replace the external commands `basename` and `dirname`:**

```
basename MYPATH
```

**or**

```
${MYPATH##*/}
dirname MYPATH
```

**Or**

```
${MYPATH%/*}
```

**If you need to check whether a filename has imbedded spaces or other special characters, use the class matching available in tr.**

**You can remove all the 'normal' characters and if anything is left, the filename contains special characters:**

```
[ "$(echo "$MYNAME" | tr -d '[:alnum:]')" != "" ] \
  && echo "filename $MYNAME has non-alphanumeric chars"
```

### Changing strings with special characters like ESC

**When writing scripts where random words must be highlighted, sed and awk will have problems with the ESC character.**

**This might be a conditional test where values larger than a certain number need to be highlighted.**

**This is the generalized sed method:**

```
echo "somestring" | sed 's/string/new_string/g'
```

**but in sed, the escape character cannot be easily used. However, Perl has no restrictions:**

```
echo "somestring" | perl -pe 's/string/any_old_string/g'
```

**The advantage with perl is that the string can include control characters such as escape.**

**On the command line:**

**type `ctrl-V` then the special char like escape**

**You'll see `^[` dropped in by the shell indicating that an escape character is now inserted in the string.**

```
echo "abcxyz123" | perl -pe "s/xyz/^[&dBxyz^[&d@/g"
```

**`ESC & d B` is the inverse video (bold) enhancement for HP terminals.**

**Better yet, use of `tput` also works.**

```
echo "abcxyz123" | perl -pe "s/xyz/$(tput bold)xyz$(tput sgr0)/g"
```

## Mail attachments

**You can use mailx to send attachments -- use ux2dos, uuencode and -m in mailx:**

```
ux2dos some_file | uuencode attachment.txt \
| mailx -m -s "some subject" somebody@somewhere.com
```

**For multiple attachments:**

```
(ux2dos file1 | uuencode file1.txt; \
 echo; ux2dos file2 | uuencode file2.txt) \
| mailx -m -s "subject stuff" <some_addr>
```

**Or better yet, use a 'here' document and add comments into the body of the message:**

```
mailx -m -s "This is the subject" bill.hassell@fiserv.com << EOF
$(ux2dos /etc/profile | uuencode MyProfile.txt)
$(ux2dos /etc/hosts| uuencode MyHosts.txt)
$(ux2dos /etc/inittab| uuencode MyInittab.txt)

So there are 3 files here.



The uuencode filename is not local to your system,

it is used to provide a title for the attachment.

You can put lots of comments here or even

use a text file like this:


$(cat /etc/nsswitch.files)



    This is the end...

EOF
```

Or use mutt (requires a valid `.muttrc` in `$HOME`)

```
mutt -a some_file -s "subject" -F /path/.muttrc <some_addr>
```

## All about EPOCH time:

Epoch time in Unix is defined as seconds since Jan 1970 (Unix birth). Conversion both ways is very useful to compute elapsed time between dates.

**- epoch seconds**

```
perl -le 'print time'

1189106293
```

**- epoch seconds back into date**

```
perl -le 'print scalar localtime(time)'

Thu Sep  6 15:17:46 2007

- any number of seconds back to date

perl -le 'print scalar localtime(86400)'

Thu Jan  1 19:00:00 1970

- using adb to decode seconds:

echo "0d1189106372=Y" | adb

2007 Sep  6 15:19:32
```

## Are Your Indexed Files Really Contiguous?

From Robert Atkinson

Having worked on OpenVMS systems for almost 20 years, I thought I had a fairly good handle on FDLs and how they worked, but I came across something recently that made me stop and think.

There's a particular file on our system that's converted daily and has the BEST_TRY_CONTIGUOUS flag set in the FDL. On checking the file headers ($ DUMP/HEADER), I found that it's very rarely contiguous. To start off with, I blamed this on the disk defragger we're running, but that was a red herring.

Finally, I found this in the OpenVMS Record Management Services Reference Manual-

*"Contiguous best try; indicates that the file is to be allocated contiguously on a 'best effort' basis..... Note that this option is ignored if multiple areas are defined for an indexed file."*

As most of our indexed files do have multiple areas, it would seem that setting this indicator is fairly pointless.

So, beware. You may think you're asking for a contiguous file, but RMS may not actually give you one.

## Data Networking and Storage Networking - hpUG Event – 4 October 2007

Data networks and storage networks behave in similar ways. It is important to understand the underlying principles thoroughly, especially when designing and implementing critical infrastructure projects that rely on these technologies.

This seminar discussed the various components involved in implementing networks and explained why they work as they do, thus helping to develop an understanding of their capabilities and limitations.

The seminar covered physical infrastructure (eg: cabling, fibre-optics), segmentation methods (eg: switching, VLANs, Zones and routing), network protocols (eg: TCP/IP, DECnet, and Fibrechannel) and performance aspects (eg: latency, bandwidth and multiple paths).

The seminar concentrated on ethernet (data networking) and fibrechannel (SAN or storage area networking) technologies, but also covered other topics such as high performance inter-site links and wireless networks.

A typical mixed system split site infrastructure design was used as a practical example of how the networks, systems and storage subsystems can be configured to provide secure internal and external access, high availability and data replication between sites.

Slides can be found at:

www.xdelta.co.uk/seminars

and at:

http://www.hpug.xdelta.co.uk/

For information about future hpUG events please see:

http://www.hpug.org.uk/index.php?option=com_events&Itemid=45

## Busting the Blade Myths

How long does it take your team to deploy a new server? How many of your administrators are involved every time? How many cables and switches do you manage? If your answer was too long or too many — take a closer look at Virtual Connect for the HP BladeSystem.

Today, most server interconnect choices come with compromises – too many cables or too much to manage. Virtual Connect cuts the network cables and eliminates the management, but adds the unique ability to wire everything once, then add, replace or recover servers in minutes versus hours or days.

IDC wrote a great report about the value of Virtual Connect that explores how it can lower costs, simplify networks or streamline daily operations.

Today, two Virtual Connect choices are available for Ethernet or Fibre Channel networks. Fully compatible with your favourite network standards and brands, Virtual Connect modules are surprisingly simple to implement but will transform the way your administrators work together.

BENEFITS OF VIRTUAL CONNECT

.. Simplify networks: Reduce your cables 94% without adding switches to manage

.. Simplify server connections: Separate your server LAN & SAN management and free your administrators from the time-consuming demands of server changes

.. Change servers in minutes, not days: Wire-once and add, replace and recover servers without affecting LANs or SANs.

## HP CORE LAN SWITCH SIGNALS RISE OF PROCURVE

The ProCurve helped HP beat Nortel Networks to become the second-biggest enterprise Ethernet switch vendor in the second quarter.

Hewlett-Packard isn't yet a household name in enterprise LANs but it is poised to extend its gains against leader Cisco with a new core switch and coordination with HP's consulting arm.

Full article available at:

http://newsletter.infoworld.com/t?ctl=196BFE7:9107B0F8CA93EBA242E4DF2DE782DEE1EFF29049075316B4

## Transoft now provides Graphical Interfaces for HP e3000 MPE/iX - as well as on Windows, Linux and UNIX

Transoft, specialists in modernisation and migration for over 20 years, now provides various graphical interfaces to VPLUS screens on HP e3000 systems via its Transoft Graphical Adapter (TGA). Until recently TGA offered an emulation of the VPLUS intrinsics on Windows, Linux and UNIX. TGA has extended the standard VPLUS functionality to allow for a Browser based user interface (ASP.NET or JSP) or a VB.NET user interface as well as the standard character terminal user interface. These graphical interfaces are now available directly on the HP e3000.

This is all possible with no changes to the VPLUS intrinsic calls in the application. VPLUS formspec files are converted to TGA XML format using a fully automated tool in the Transoft Legacy Liberator IDE.

Using the TGA Client generation tool, the TGA XML files are used to generate the required user interface source code which may be ASP.NET pages, JSP pages or VB.NET forms.

The TGA XML files are copied to the platform on which the application is running so that they can be read by the TGA library at runtime.

On HP e3000 the TGA library (TGAXL) is linked to the application to provide the TGA emulation of the VPLUS intrinsics. The application may be written in COBOL, HP BASIC, Pascal; any language in which the VPLUS Intrinsics may be used.

The TGA Broker runs as a background job, listening for connections from TGA client applications. When a TGA Broker receives a graphical client connection it starts the VPLUS application according to details set in a configuration file and starts a new job which runs the application and communicates directly with the TGA client application.

The user environment can be set up so that it is equivalent to the environment for standard user sessions on HP e3000.

For more information on Transoft's software and service solutions for the HP e3000 environment please visit:www.transoft.com/hp3

Please also see the following diagram: www.hpug.org.uk/e-ping/Tga_deploy_mpe.jpg

and screen shots:

Tga-charterm is a screen shot of a VPLUS app in a terminal emulator: www.hpug.org.uk/e-ping/Tga-charterm.jpg

Tga-aspnet is a screen shot of a VPLUS app in a browser - exactly as generated automatically - no changes to page layout: www.hpug.org.uk/e-ping/Tga-aspnet.jpg

Tga-aspnet2 is a screen shot of a VPLUS app in a browser with a few changes to style sheets and slightly modified page layout - to give an idea what can be done quickly: www.hpug.org.uk/e-ping/Tga-aspnet2.jpg

## News from Novell

Novell Announces Real-Time Linux Enhancements and Partnerships Press Release - http://www.novell.com/news/press/novell-announces-real-time-linux-enhancements-and-

partnerships/?sourceidint=ic_nb062107_slert

The openSUSE Project Turns Two with Improved Build Service and 10.3 Beta Press Release

http://www.novell.com/news/press/the-opensuse-project-turns-two-with-improved-build-service-and-10-3-beta

Novell Ships SUSE Linux Enterprise 10 Service Pack 1 and New Virtual Machine Driver Pack –

http://www.novell.com/news/press/novell-ships-suse-linux-enterprise-10-service-pack-1-and-new-virtual-machine-driver-pack/?sourceidint=ic_nb062107_sp1

Bringing More Applications to Linux - Jeff Jaffe discusses ways to enlarge the ISV ecosystem –

http://www.novell.com/ctoblog/?m=20070813

Your Linux is Ready for Quad-Core AMD Opteron Processors –

With the launch of Quad-Core AMD Opteron processors, SUSE Linux Enterprise Server is the first and only Linux Distribution to support AMD's latest key innovations:

http://www.novell.com/virtualization/opteron/

Virtualization from Novell Built to Innovate –

Virtualization from Novell is the leading open source solution for Windows server consolidation, rapid provisioning and high availability. This integrated solution brings it all together:

http://www.novell.com/virtualization/

Novell-led Bandit Project Launches 'Control Your Identity' Campaign –

To drive better, more secure user management of Internet identities, the Novell-led open source Bandit Project has kicked off the “Control Your Identity” campaign, to promote awareness and use of information card technology.

Read the full article:

http://www.novell.com/news/press/novell-led-bandit-project-launches-control-your-identity-campaign/

## Golddust - Competition to find the Oldest Working Server

The winner of the oldest server competition was Geoff Butler of Oxford University Press. He was presented with a new HP server and an HP camera by Pete Murray, Director Enterprise Servers and Storage, HP UK&I. It was stated in the meeting that the new server was in the order of 200 times faster than the one that won the competition.

The three finalists were Geoff Butler of Oxford University Press, Peter Windle of Apollo Fire detectors and Lyndon Hepworth (for Guy Humphreys) of Celanese Acetate Products.

Guy Humphreys from Celanese Acetate was the HP User group member who entered and was shortlisted. Lyndon Hepworth attended on his behalf as Guy was on holiday.

For more details and photo, please see: www.hp.com/uk/golddust

### The HP Servers at Celanese Acetate Products Ltd

Celanese Acetate is a multinational manufacturer of cellulose acetate products. The UK division, previously known as Acetate Products and before that was part of Courtaulds Acetate, primarily manufactures cigarette filter tips for a large number of cigarette brands around the world. The UK

division operates from two manufacturing plants, the largest of which is staffed by around 800 people in Spondon, Derbyshire. Because the site deals with a very large volume of international orders it has to be up and running 24 hours a day, seven days a week.

The company has been using HP servers and the HP-UX operating system since the 1980s when it was still part of Courtaulds Acetate. Its oldest surviving HP-UX server is a model dating back to 1993.

It chose the HP server and operating system for its extreme reliability and stability, says Guy Humphreys, senior business analyst at Celanese Acetate: “The manufacturing operation is 24/7 and we need the servers to be up the entire time. If we have any downtime it would cost us a lot in terms of time and efficiency. The whole manufacturing process is run by the HP servers. For example, they handle all the product labelling and we simply couldn’t do without that.”

The company’s first HP-UX servers were able to take on the Enterprise Resource Planning (ERP), inventory, finance and stock control applications and run a large database full of vital customer and process information.

Since splitting from Courtaulds Acetate, Celanese Acetate’s IT department has also become a services provider for different businesses that were once formerly attached to the company.
In running such a large number of mission-critical applications for its own operation as well as housing outsourced applications, it was important that the servers could be partitioned effectively. “HP-UX is particularly good at working with Logical Volume Manager (LVM), which ensures we make the best use of our disk space, and provides essential resiliency and storage performance,” says Humphreys.

Since the 1980s the business has been through many changes but its need for a reliable and scalable solution has remained the same. It has been through a number of hardware refreshes and now runs HP-UX on 12 HP 9000 servers, which deal with all the company’s mission-critical applications. Although the HP 9000 server dating from 1993 no longer runs mission-critical applications, it’s still up and running.

“We haven’t touched the old server in years,” explains Humphreys. “The great thing about HP-UX is that it’s rock solid, which is why we haven’t felt the need to move to any other operating system. You can just leave the servers running and they need minimal attention and maintenance and you know they won’t let you down. They’re as solid as a brick.”

## Worldwide User Advocacy Survey Captures Enterprise HP Customer Feedback

Over the past year leading independent HP users groups Encompass, HP-Interex EMEA, ITUG, and Encompass Asia-Pacific partnered with HP to produce the 2007 Worldwide User Advocacy Survey. Implemented and advertised by the international HP user group community, this 18th annual survey was conducted between May 2nd and July 2nd and captured input from over 1100 individual respondents.

### The Survey

Similar to the 2006 survey, the 2007 HP Worldwide User Advocacy Survey was designed with two major objectives: to measure customer perceptions of HP enterprise products and services, and to seek user input on future product features and enhancements. The volunteer committee representing HP’s prominent international users groups commissioned Spring Incorporated, an independent research firm, to construct the survey and analyze the data captured.

To expedite the survey process and ensure the most qualified results, respondents were asked to provide input related only to those product(s) most familiar and important to them. Enterprise HP products featured in the survey included HP-UX, OpenVMS, NonStop, Open Source, Linux, and Tru64 UNIX. The committee also included a section specifically to capture input about and from HP partners and resellers.

### The Message

The worldwide user and partner community generally rated HP products and technology highly, both on individual product merits as well as relative to competitive offerings. With few exceptions, users conveyed high quality ratings and strong degrees of loyalty for the HP product sets they use.
Both users and partners expressed interest in HP making it easier to do business during the sales process. HP has work going on to simplify the business to business processes and will work with the user groups to further understand the survey comments and drive improvements to processes and experiences.

### What Now?

The committee of user group representatives presented an executive summary of survey results and recommended next steps to over 160 HP executives, managers and development team members in late August. This information has been circulated to additional HP product teams and decision-makers through subsequent presentations by both user group representatives and HP employees.

Participating user groups are utilizing the survey results to enhance advocacy efforts through follow up surveys and deeper dives into areas of particular interest.

The survey committee would like to thank the users and partners who took the time to complete the survey; your feedback was heard and the collective product of your effort is currently being used to enact positive change with HP. Watch the Web sites of Encompass, HP-Interex EMEA, ITUG, and Encompass Asia-Pacific for details as they are announced.

## Ulink - HP-Interex EMEA Weekly E-Newsletter

Please visit http://www.hp-interex.org/ulink to view the latest newsletter

## Hints and Tips

from Bill Hassell

### How to log TCP and UDP connections in HPUX

PROBLEM

By default HPUX does not log every tcp and udp connection. If there is a desire to log that information the program Ipfilter can be used. Please be aware that logging all of these types of connections can create extremely large amounts of log data.

RESOLUTION

The software Ipfilter is provided by HP as a free download for HPUX 11.00 and HPUX 11.11. For HPUX 11.23 the software product is pre-installed with the operating system. IPfilter is highly configurable, this document is only addressing how to enable logging for tcp and udp packets. For more detailed information on how to configure IPfilter please reference the user manuals available on the following web site. http://www.docs.hp.com/en/internet.html

The software can be downloaded at the following web site.

https://h20293.www2.hp.com/portal/swdepot/try.do?productNumber=B9901AA

To enable logging of UDP and TCP packets and allow all traffic in and out of your system perform the following steps:

1. Add the following lines to the /etc/opt/ipf/ipf.conf configuration file.

```
pass in log first quick proto tcp from any to any flags S keep state
pass out log first quick proto tcp from any to any flags S keep state
pass in log first quick proto udp from any to any keep state
pass out log first quick proto udp from any to any keep state
pass in from any to any
pass out from any to any
```

2. Load the configuration file.

```
# /sbin/ipf -f /etc/opt/ipf/ipf.conf
```

Once the configuration is loaded every time a UDP or TCP connection is initiated it will be logged to the /var/adm/syslog/syslog.log.

Here is an example of the syslog messages generated:

```
Jul 22 08:16:05 gator ipmon[821]: 08:16:04.761394 lan0 @0:2 p
15.17.188.178,65473 -> 15.17.191.255,111 PR udp len 20 152  K-S IN
Jul 22 08:16:07 gator ipmon[821]: 08:16:06.521399 lan0 @0:2 p
15.17.186.112,123 -> 15.17.186.215,123 PR udp len 20 76  K-S OUT
Jul 22 08:16:10 gator ipmon[821]: 08:16:09.771417 lan0 @0:2 p
15.17.188.178,65474 -> 15.17.191.255,111 PR udp len 20 152  K-S IN
Jul 22 08:16:11 gator ipmon[821]: 08:16:10.481417 lan0 @0:1 p
15.228.73.123,3028 -> 15.17.186.112,1570 PR tcp len 20 48 -S K-S IN
Jul 22 08:16:12 gator ipmon[821]: 08:16:11.491422 lan0 @0:1 p
15.228.73.123,3029 -> 15.17.186.112,23 PR tcp len 20 48 -S K-S IN
Jul 22 08:16:12 gator ipmon[821]: 08:16:11.531422 lan0 @0:2 p
15.17.186.112,49204 -> 15.51.240.8,53 PR udp len 20 72  K-S OUT
Jul 22 08:16:12 gator ipmon[821]: 08:16:11.541427 lan0 @0:2 p
15.17.186.112,49205 -> 15.51.240.8,53 PR udp len 20 78  K-S OUT
Jul 22 08:16:16 gator ipmon[821]: 08:16:15.261441 lan0 @0:2 p
15.17.186.130,138 -> 15.17.191.255,138 PR udp len 20 229  K-S IN
Jul 22 08:16:22 gator ipmon[821]: 08:16:21.551473 lan0 @0:2 p 15.17.184.47,138 -
> 15.17.191.255,138 PR udp len 20 229  K-S IN
Jul 22 08:16:22 gator ipmon[821]: 08:16:21.851473 lan0 @0:2 p 15.17.184.47,137 -
> 15.17.191.255,137 PR udp len 20 78  K-S IN
Jul 22 08:16:31 gator ipmon[821]: 08:16:31.061514 lan0 @0:2 p
15.17.191.134,138 -> 15.17.191.255,138 PR udp len 20 229  K-S IN
Jul 22 08:16:31 gator ipmon[821]: 08:16:31.061516 lan0 @0:2 p
15.17.187.226,138 -> 15.17.191.255,138 PR udp len 20 229  K-S IN
Jul 22 08:16:31 gator ipmon[821]: 08:16:31.061518 lan0 @0:2 p
15.17.187.218,138 -> 15.17.191.255,138 PR udp len 20 229  K-S IN
Jul 22 08:16:31 gator ipmon[821]: 08:16:31.081514 lan0 @0:2 p 15.17.186.60,138 -
> 15.17.191.255,138 PR udp len 20 241  K-S IN
Jul 22 08:16:36 gator ipmon[821]: 08:16:35.961537 lan0 @0:2 p
15.17.187.219,138 -> 15.17.191.255,138 PR udp len 20 229  K-S IN
```

### HP-UX TCP TimeStamp option with "wraparound" results in dropped packets

PROBLEM

If the TCP TimeStamp option is used, when a TCP connection receives wraparound TimeStamp values from peer, it begins to drop received packets.  Finally, the TCP connection will be dropped.

Note: The TimeStamp value is 32 bit. The "wraparound" feature occurs when this value grows to 0xffffffff; it will then start from 0 again.

On HP-UX 11.x, the lbolt value is used as a TimeStamp value, so the problem will occur if the system has been on for a long enough period of time.

How can this problem with the dropped packets and dropped TCP connection be resolved?

CONFIGURATION

Operating System - HP-UX
Version - 11.X
Subsystem - ARPA Transport

RESOLUTION

The following is taken from the second paragraph of section 4.2 of RFC 1323:

"In both the PAWS and the RTTM mechanism, the "timestamps" are 32-bit unsigned integers in a modular 32-bit space. Thus, "less than" is defined the same way it is for TCP sequence numbers, and the same implementation techniques apply. If s and t are timestamp values, s < t if 0 < (t - s) < 2**31, computed in unsigned 32-bit arithmetic."

HP's current implementation does not consider the right side condition (t-s) < 2**31, so, it mistakes the wraproud as an outdated timestamp. Due to the PAWS algorithm, segments received with an outdated timestamp should be rejected. This is why the problem occurs. (Reference section 4.2.3 of RFC 1323.)

To work around this issue, disable the TCP TimeStamp option by turning the ndd tunable tcp_ts_enable to 0.

This problem has been reported to the proper lab, but a General Release patch is not available at the time of this writing. It is recommended to periodically check HP's ITRC web site at: http://www.itrc.hp.com for new patch releases or open a support call with your local HP Support Center for more assistance.

## HP-UX Secure Shell (ssh) A.03.90 supports TCP Wrapper language extensions

PROBLEM

The HP-UX Secure Shell (ssh) A.03.81.002 does not support the TCP Wrappers optional language extensions.

CONFIGURATION

Operating System - HP-UX
Version - 11.11, 11.23
Subsystem - Secure Shell (ssh)

RESOLUTION

HP-UX 11.23 is configured to use TCP Wrappers in the standard OS and it uses a shared library with the language extensions compiled in.

The HP-UX Secure Shell (ssh) version 3.9 has been enhanced to support TCP Wrapper language extensions.

Also, please see:

Doc_id: 8606387136
Title: Would like for sshd to use hosts options lang extensions from libwrap

available at: http://www.itrc.hp.com

## SYS ADM: what TCP ports enable remote printing; HP-UX to NT print server

PROBLEM

An NT computer is configured as a printer server that will receive requests from an HP-UX computer.

What TCP ports need to be opened to enable remote printing through a firewall?

CONFIGURATION

Operating System - HP-UX
Subsystem - lpr

RESOLUTION

Line Printer Daemon Protocol (LPR) is a protocol for communications between clients that want to print documents and servers that host the printers. If the servers are Unix-based, the LPR protocol is handled by the Line Printer Daemon (LPD). Under Windows, a service called the Windows NT LPD Server is used. The LPR protocol is discussed in the Internet Engineering Task Force RFC 1179, entitled:

"Line Printer Daemon Protocol" available at: http://www.rfc-editor.org/rfc/rfc1179.txt

LPR is a simple protocol that is carried by TCP. The first octet of an LPR command specifies the function and is followed by the ASCII name of the printer queue on which the function is to be performed. Any further operands to the command are separated from the printer queue name with white space (ASCII space, horizontal tab, vertical tab, and form feed), and the end of the command is an ASCII line feed character. See the RFC for a command list.

RFC 1179 specifies TCP ports 721 through 731 for inbound and outbound connections to the LPD service which handles LPR. NT 3.51 introduced RFC-compliant LPR support to Windows. See "Updated TCP/IP printing components for Windows NT 3.51" at the following URL: http://support.microsoft.com/support/kb/articles/Q153/6/66.ASP

This was the standard until the release of NT 4.0 Service Pack 3, when the service defaulted to TCP ports in the 512 to 1,023 range. See "Updated TCP/IP printing options for Windows NT 4.0 SP3 and Later" at the following URL: http://support.microsoft.com/support/kb/articles/Q179/1/56.ASP

Service Pack 3 can also be configured through two registry entries to enable the use of TCP ports 1,024 and greater.

Why did they change from the RFC definition of LPR?

When Windows used TCP ports 721 through 731 for LPR connections, it limited performance because this configuration only allowed 11 TCP ports to be used simultaneously. Worse still, according to RFC 1122:

"Requirements for Internet hosts - communication layers"

a TCP port must not be reused within four minutes except when a remote computer reopens a previously closed connection. This is discussed in the Microsoft Knowledge Base article "Printing to LPD printer is slow or fails with Windows NT" at the following URL: http://support.microsoft.com/support/kb/articles/Q141/7/08.ASP

Rather than change the protocol to a proprietary one, Microsoft chose to make more ports available - ports 512 through 1,023. While this improves performance for Windows clients, Microsoft notes that the increased port range "causes problems with some applications" because non-Windows clients might consider getting an LPR response from a server on a nonstandard port to be an error - and quite rightly so.

## HP-UX TCP/IP - What TCP (or UDP) Port Numbers Should My Application Use?

ISSUE

I am trying to determine what various TCP ports numbers are used for. I am developing my own application and do not want to use a port number that is already used.

SOLUTION

The following information generally applies to both TCP and UDP ports.

There are, in fact a few different port ranges that we might be concerned with:

1) Reserved ports (0-1023)
2) Registered ports (1024-49151)
3) Legacy (10.20 and before) "anon" ports (1024-5000)
4) Current (11.0 and later) "anon" ports (49152-65535)

The first range, reserved ports, are those ports that will be used by programs that need a special privilege to get the ports such as telnet and ftpd. This range is fixed by the TCP specifications and does not change. These port numbers are only available to applications running as "root".

The second range are the "Registered Ports" and are available for applications to use. This is, in general the rage that you will be drawing from. Individuals and Companies may register the use of these ports with the "Internet Assigned Number Authority (IANA) but do not need to.

The next two ranges are actually very similar. These are the ranges of port numbers that will be handed out by the HP-UX system when an application needs a port number but has not explicitly requested a specific one. So for instance, when you make a TCP connection TCP will allocate a local port number from this range and assign it to your local socket. Likewise, if you make the bind(2) system call with the port number set to 0 then TCP will allocate a port out of this range and assign it to your socket. This is also called the ephemeral port range or the dynamic port range.

In HP-UX versions 10.20 and older this range was 1024-5000 which conflicts with the IANA Range. Starting with HP-UX 11.0 this range moved to the range 49152-65535. It is actually tunable via the ndd(1m) command. You may adjust the lower bound using the ndd option "tcp_smallest_anon_port". For this reason it makes sense typically to allocate port numbers between 5000 and 6000 or in a range such as 10,000 to 20,000. Remember that X11 uses TCP port numbers 6000+display number, so avoid 6000-6010.

For a more detailed listing of "Well Known Ports" see: http://www.iana.org/assignments/port-numbers

You will find that there are a very large number of ports assigned to various services (Registered) but most are not in common use. It is also the case that port numbers should never be hard-coded into an application. Instead the application should use a unique "service name" and then call getservbyname(3N) with that name to get the port number they should use. The mapping between the unique service name and the TCP or UDP port number is then done in /etc/services and thus can easily be changed to accommodate the needs at a specific installation.

## HP-UX - 'tcp_lift_anchor, can't wait' TCP RST reset messages occur in application log

ISSUE:

HP-UX 11.x servers running a third party application experience mass socket closure and DSS connection loss in node/node and node/client communication. Application logs include many "tcp_lift_anchor, can't wait" with TCP RST reset messages.

What causes "tcp_lift_anchor, can't wait" TCP RSTs and how can they be stopped?

SOLUTION

Only an application can control when the close on a listen socket occurs. If the application performs quick closes on listen sockets while the peer systems are initiating connects at the same time, then the tcp_lift_anchor() RST can occur.

HP's TCP implementation sends this RST because we feel that it is appropriate to notify the client that their connect request will never be serviced because the listen socket was closed by the server's application.

As of the date of this writing, there is not a way to stop the RST when this condition occurs. No tunable is available to turn the tcp_lift_anchor() RST off because the TCP implementation was designed to inform the peer that the connect request will not be serviced under the conditions described above.

### HP-UX 11.0 - Reset cause: tcp_eager_blowoff, "can't wait" message from TCP resets

PROBLEM

On an HP-UX 11.0 system, several TCP resets occur with the following reason:

Reset cause: tcp_eager_blowoff, "can't wait"

CONFIGURATION

Operating System - HP-UX
Version - 11.0
Subsystem - ARPA Transport

RESOLUTION

The TCP resets with the message shown above occurs when a server application hits the value of the "maxfiles" kernel tunable. When the "maxfiles" value is hit, then the sogetfile() system call, called from soaccept(), fails and the error handling leads to soabort1() which results in the transmission of a TCP RST (payload reason of "tcp_eager_blowoff, can't wait").

In other words, the Server accept() system call is failing with:

[EMFILE] The maximum number of file descriptors for this process are currently open.

### HP-UX NFS - NFS Server Not Responding or Process Hangs Over NFS Mounts

ISSUE

The NFS application will typically display one of the following NFS Warning Messages:

NFS Server Not Responding ...
vmunix: NFS write failed for server ...

The first example is for hard mounts (default) and the second for soft mounts.

NFS HARD VERSUS SOFT MOUNT BEHAVIOR

There are a few differences between soft and hard mounts. Most notably NFS Soft mounts will time out if there is a problem communicating with the NFS server. NFS Hard mounts will hang or retry until communication issues with the NFS server are resolved.

SOLUTION

Many times the root cause(s) of NFS hangs or timeouts may not be NFS, but rather an issue with underlying network, a system resource problem or I/O bottleneck with any one of the many subsystems NFS depends upon. Issues could be on the NFS client, the network, or on the NFS server.

We would recommend asking a few questions before performing extensive NFS debugging.

Did this ever work?
If it did work, WHAT HAS CHANGED?
Network
Load on systems
Disk / Storage
Patches

Was something else happening at the time?

Does the problem happen at the same time of day?

Does the NFS Server Not responding message appear frequently, or just a few entries at a time or rarely?

Are many clients getting the same messages about the same server?

Is the NFS Server not responding for just one filesystem exported by the NFS Server or for all of them?

The following steps will assist you with troubleshooting the most common causes for NFS communication issues.

NOTE: For further information on all the commands referenced in this document consult the relevant man pages.

Troubleshooting Steps to follow:

CHECK THE NETWORK

It is best to begin by checking the overall health of the network and the server.

ping

Use the "ping" command to test communication to the server with 8000 byte packets - is there any packet loss?

# /usr/sbin/ping nfs-server 8000

To see the ping results, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_ping_results.txt

In the above example, you can see that some of the ping packets are not acknowledged. Packet loss could contribute to the NFS issue!

traceroute

Use the "traceroute" command to check the routing path to the server to see where packet loss or delays may be occurring.

# /usr/contrib/bin/traceroute nfs-server.hp.com

To see the traceroute results, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_traceroute_results.txt

The above example shows no delays since all responses are under 100ms.

The traceroute command could show that packets are taking an unexpected path to or from the server which could account for time lapses or unexpected network bottlenecks.

Example of a problem reaching a host:

# /usr/contrib/bin/traceroute 192.168.20.101

To see the example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_traceroute_example.txt

Possible causes could be mis-configured routes to the other host, router issues, cable or network issues beyond the router cisco-1.test.com

NOTE: You may need to specify the network PPA# with the -I option for the traceroute command.

Example using lan2 as the interface for traceroute.

# /usr/contrib/bin/traceroute -I 2 nfs-server.hp.com

Check the nettl log file
Check the nettl log on the NFS client, and on the NFS server for cable disconnection, duplicate IP issues, or other recent issues.

Format the nettl log file as follows:

# /usr/sbin/ netfmt -f /var/adm/nettl.LOG000 > netlog000.out

To see the nettl log example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_nettl_log.txt

Check lanadmin statistics for all LAN NICs used with NFS

The interface used for NFS traffic is dependent on IP routing, use the "netstat -rn" command to determine which interfaces are used to route your NFS traffic.

root@nbox# /usr/bin/netstat -rn

Routing tables

Destination Gateway Flags Refs Interface
Pmtu 127.0.0.1 127.0.0.1 UH 0 lo0 16424 16.113.145.130 16.113.145.130 UH 0
lan0 16424 192.15.15.178 192.15.15.178 UH 0 lan2 16424 192.15.15.0 192.15.15.178 U 2
lan2 1400 16.113.144.0 16.113.145.130 U 2 lan0 1500 127.0.0.0 127.0.0.1 U 0 lo0 0
default 16.113.144.1 UG 0 lan0 0

Use the "netstat -in" command to review the Input and Output packets along with any errors or collisions.

Example of a problem on a 100BaseT card:

# /usr/bin/netstat -in

Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
lan2 1500 192.15.15.0 192.15.15.178 8220 0 16404 0 0
lan0 1500 16.113.144.0 16.113.145.130 1456126 2981 1182378 0 0

Above, there are indications of an issue on lan0 due to the Ierrs noted.

The LAN interface number (LAN#), which is also known as the PPA number, can be used to review detailed information about the interface.

Use the "lanadmin" command to check the detailed statistics.

Example using lanadmin to view lan0 information.

# /usr/sbin/l anadmin -g 0

To see an example of a problem on a 100BaseT card, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_100BaseTCard_problem.txt

NOTE: FCS or CRC framing errors are often caused by duplex mismatches. Double check the network configuration.

The "lanadmin -x ppa#" command can be used to check the speed, duplex and negotiation status of the card.

NOTE: For Gigabit links use "lanadmin -x card_info PPA" to get the link status.

# /usr/sbin/lanadmin -x 0

Current Config = 100 Half-Duplex AUTONEG

In the above case, the HP interface is set to 100 Half Duplex. The existence of  Collisions and FCS errors may indicate a duplex mismatch between the HP NIC and the switch port. Correct the duplex mismatch, if any, and see if the NFS problems go away.

Example of a Gigabit link down:

# lanadmin -x 13

To see the example of a Gigabit link down, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_Gigabit_link_down.txt

Verify the CLIENT can communicate to the NFS Server processes. From the Client, use the "rcpinfo" command to test RPC layer communication to the NFS Server.

First, see if the mountd and nfsd programs are registered with rpcbind on the NFS Server, the -p option to rpcinfo prints the programs that have registered with the rpcbind program.

# /usr/bin/rpcinfo -p nfs-server

Second, try to "ping" the rpc.mountd and nfsd processes with these 4 commands:

NOTE: The -u option tests the UDP protocol, the -t option tests the TCP protocol.

# /usr/bin/rpcinfo -u nfs-server mount
# /usr/bin/rpcinfo -t nfs-server mount
# /usr/bin/rpcinfo -u nfs-server nfs
# /usr/bin/rcpinfo -t nfs-server nfs

Examples:
# /usr/bin/ rpcinfo -p nfs-server program vers proto port service

To see the rpcinfo examples, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_rpcinfo_examples.txt

See if the NFS client can see the exports list of the NFS Server:
# /usr/sbin/showmount -e nfs-server

For example:
# /usr/sbin/showmount -e nfs-server

To see this example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_rpcinfo_examples.txt

Verify the export list is correct. If not, log into the server and examine the /etc/exports file. If it contains entries that you do not see in the showmount -e listing, then re-export them as follows:
# /usr/sbin/exportfs -av

For example:
# /usr/sbin/exportfs -av re-exported /home

To see the re-export example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_exportfs_example.txt

See what files the NFS Client has mounted from the NFS Server:

NOTE: CAUTION! If you use "bdf" it causes an NFS "fsinfo" request to the NFS Server, which can cause the bdf command to hang if there are any problems! Use the "mount" command instead.

# /usr/sbin/ mount

Or if you have a bunch of filesystems:

# /usr/sbin/ mount | egrep -I 'nfs|autofs'

For example:

# /usr/sbin/mount | egrep -I 'nfs|auto'

/testhack on /etc/auto.direct ignore,direct,dev=5f000001 on Wed Dec 13 09:33:28 2006
/mnt on vick1:/tmp rsize=32768,wsize=32768,NFSv3,dev=5f000005 on Tue Feb 6 15:21:41 2007

:ALTERNATIVELY

# cat /etc/mnttab

or

# egrep -I 'nfs|autofs' /etc/mnttab

Use the "nfsstat" command to view the statistics on the NFS client nfsstat -m on the client

Tip: put in background mode if dealing with hung NFS mounts points

The command "nfsstat -m" shows the mount options and general statistics for each individual mount.

General Guidelines:

srtt: Smoothed round-trip time. If this number is larger than 50ms, the mount point is slow.

dev: Estimated deviation.

cur: Current backed-off timeout value.

Lookups: If cur>80 ms, the requests are taking too long.

Reads: If cur>150 ms, the requests are taking too long.

Writes: If cur>250 ms, the requests are taking too long.

For UDP (connectionless) mounts, the most important statistic is the Service Round Trip time (srtt). If the times are excessive this could indicate a network problem or other system resource bottlenecks - Disk, SCSI, CPU, Memory.

Example UDP output:

To see the UDP output example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_UDP_output.txt

# /usr/bin/nfsstat -m &

For TCP (connection-oriented) mounts, these statistics are typically 0ms since NFS relies upon the TCP protocol to manage the communication timers.

Review the "netstat -s -p tcp" output for TCP statistics.

Example output for TCP:

# /usr/sbin/ nfsstat -m &

To see the TCP output example,
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_TCP_output.txt

nfsstat -c on the client

The "nfsstat -c" command displays client information. Only the client side NFS and RPC information will be printed. You will likely see some timeouts on the client side. You will see these increasing when "NFS Server not responding" or NFS hangs/timeouts occur.

TIP, the most important statistics are the badxid, retrans and timeouts.

badxid The number of times a reply from a server was received which did not correspond to any outstanding call.

retrans The number of times a call had to be retransmitted due to a timeout while waiting for a reply from the server.

timeout The number of times a call timed out while waiting for a reply from the server.

Here are some helpful hints:

If the timeout and retrans values displayed by nfsstat -c are high, but the badxid value is close to zero, packets are being dropped before they get to the NFS Server. Try decreasing the values of the wsize and rsize "mount" options to 1024 on the NFS client as a workaround to the underlying network problem.

If the timeout and badxid values displayed by "nfsstat -c" are of the same magnitude, your server is probably slow or overloaded. Client RPC requests are timing out and being retransmitted before the NFS server has a chance to respond to them.

Verify the network is not the cause of delay (e.g. long ping and traceroute results in Step #1).

The "nfsstat -c" command is cumulative, so repeat it to examine how statistics are changing. A look at the types of calls your NFS client is making may help you isolate the source of a performance issues as well.

Example "nfsstat -c" output:

# /usr/bin/nfsstat -c

To see the nfsstat example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_nfsstat_example.txt

Login into the NFS Server to investigate further.

Follow the procedures in Step 1 to interrogate the network on the NFS server

Check that the exported filesystems are OK and can be accessed without any problem.

Log into the NFS Server and check the exported filesystems listed in /etc/exports.

For example, use the "bdf" or "du" commands on the filesystems to make sure they can be accessed locally.

Then check for disk issues with "GLANCE" or "sar -d 1 15" looking for delayed or long avwait (wait) or avserv (service) times.

TIP on using sar -d

# sar -d [interval] [iterations]

Is %busy for any of the disks >50?

NOTE: 50% is a rough guide, a better question would be is it much higher than normal for your system. On some systems even a %busy value of 20 may indicate a disk bottleneck, while others may normally have disks that are 50% busy.

For this same disk, is avwait > avserv?
No -> Most likely no disk bottlenecks,

Yes -> There seems to be an IO bottleneck on this device.

Example sar -d 1 15 showing a disk bottleneck:

HP-UX nbox B.11.11 U 9000/800 02/09/07

To see the bottleneck example, go to
ftp://ftp.hp.com/pub/enterprise/programming_code/c00867456_disk_bottleneck.txt

If the NFS client is using UDP mounts, check for UDP Socket overflow # /usr/bin/netstat -sp udp | grep overflow 78095 socket overflows

Zero overflows indicates that there may be enough nfsd's to handle the incoming NFS calls over UDP (Connectionless). If we are running too few nfsd's, then this number may be nonzero.

Since this number is a cumulative count since the system has booted for all UDP server programs, not just NFS, you can use an option to the "ndd" command to examine which program is causing the overflows. The ports are listed in hex, since NFS uses port 2049 converting that to hex gives you "801".

Example:

# /usr/bin/ndd -get /dev/udp ip_udp_status |grep 0801

Here is an example where NFS is reporting 78095 socket overflows:

NOTE: The output of the ndd command contains many columns, we have deleted several columns for readability.
UDP ipc hidx lport <stuff deleted >
overflows <stuff deleted> 000000004258bd28 0001 0801 0000078095

Compare this value to the output of "netstat -sp udp". If there is a difference then we know that some other UDP server program may be causing the socket overflows. Review the entire output of the "ndd -get /dev/udp/ ip_udp_status" command for other programs which may be causing the overflows.

You can increase the number of available NFSD daemons dynamically on the command line. To survive a reboot you need to update the /etc/rc.config.d/nfsconf file.

# /usr/sbin/nfsd num_nfsd num_nfsd is the suggested number of file system request daemons that will start. The actual number of daemons started will be one daemon to support kernel TCP threads plus a number of UDP daemons. The number of UDP daemons started will be the value of num_nfsd rounded up to a multiple of the number of active CPUs in the system.

/etc/rc.config.d/nfsconf

NUM_NFSD=num_nfsd

Use GLANCE to examine the NFS Server for CPU, DISK, Memory or Network bottlenecks as well as NFS activity
General Guidelines:

CPU - look for 100% or very high CPU utilization

DISK - look for busy disk lvols or devices from the exported filesystems

MEMORY - Are you seeing 100% utilized or excessive swap?

Network - Are the LANs being used for NFS seeing heavy traffic?

NFS - check the NFS server by (client) system to see if an unexpected amount of traffic from another client might be causing the other client(s) to see performance issues.

Still seeing problems? Collect a nettl network trace

If we still are not able to explain the timeouts, then it may be necessary to take a network trace. It is best to do this on both the client and server at the same time during a problem period. There are some cases, due to network load, where nettl simply cannot process all the packets on the client or the server. If you have one of those cases, then we can only recommend that you use some other method of tracing, like using a network sniffer.

Start the traces on BOTH systems
# /usr/sbin/nettl -tn pduin pduout -e ns_ls_ip -tm 99999 -m 128 -f /var/tmp/raw0

NOTE: The above syntax will collect 2 50MB raw packet files at the IP layer, only collecting the first 128 bytes of each packet so the TCP/UDP and RPC headers will be captured. Use a fast filesystem for your output file (-f ), preferably one not seeing other activity. We recommend a filesystem outside of vg00.

Reproduce the problem

Once the trace is running, you would need to monitor dmesg or syslog.log for NFS warning messages or manually reproduce the problem.

When you see the problem, stop the trace as soon as possible!

Stop the trace as follows:

# nettl -tf -e all

Validate the trace files and gzip them

The "oldest" packets will be in raw0.TRC001 and the "newer" packets will be in raw0.TRC000.

Use netfmt -sf raw0.TRC00* to review a summary of the trace files.

When you have reviewed them, gzip them.

Analyze the trace files with WireShark or contact HP

Wireshark is a public domain packet collection and analysis tool that runs on PC and UNIX systems, including HP-UX. It will read the gzip'd or non-gzip'd raw nettl trace files, and has a comprehensive set of analysis functions.

For Wireshark go to http://www.wireshark.org

Click here for Wireshark:

NOTE: The previous link will take you outside the HP Web site. HP does not control and is not responsible for information outside of the HP Web site.

HP REFERENCES:

For HP NFS documentation visit HP's Technical documentation "I/O Cards and Networking Software" site.

For the HP Technical Documentation site, go to http://www.docs.hp.com/en/netcom.html

Recommended HP documentation:

NFS Services Administrator's Guide
Managing NFS and KRPC Kernel Configurations in HP-UX 11i v2
NFS Performance Tuning for HP-UX 11.0 and 11i Systems

Title: Optimizing NFS Performance: Tuning and Troubleshooting NFS on HP-UX Systems
ISBN: 0130428167

## HP-UX NFS - Can You Give Examples of NFS Mount Permission Issues?

ISSUE

When attempting to mount a Network File System (NFS) filesystem the client receives permission denied.

SOLUTION

It is worthwhile to give a brief overview of how the mountd program works and what its role is in NFS communication.

NOTE: For further information on all the commands referenced in this document consult the relevant man pages. When a NFS client attempts to mount a NFS server filesystem it will communicate initially with the following two Remote Procedure Call (RPC) programs:

rpcbind / portmapper  (/usr/sbin/rpcbind )mountd  (/usr/sbin/rpc.mountd)

What is the role of the portmapper / rpcbind programs?

When a RPC program starts it registers itself with rpcbind. The program provides its program number (mountd = 100005), the protocol the program uses (tcp, udp), the version numbers the program supports ( mountd = ver 1 & 3), and the port number the program has attached to.

When a client needs to contact a RPC program it sends a request to the rpcbind server for the program contact information. If the program has registered with rpcbind it will return a list of the current RPC program-to-address mappings. If not rpcbind returns a program not registered message.

At this point the rpcbind program is no longer involved in the transaction.

Example of rpcbind program information generated via the rpcinfo command on a HP-UX server.

```
/usr/sbin/rpcinfo -p |grep rpcbind
   program vers proto   port  service
   100000    4   tcp    111  rpcbind
   100000    3   tcp    111  rpcbind
   100000    2   tcp    111  rpcbind
   100000    4   udp    111  rpcbind
   100000    3   udp    111  rpcbind
   100000    2   udp    111  rpcbind
```

What Does rpc.mountd do on startup?

Being a good RPC citizen, when rpc.mountd starts it registers itself with rpcbind and informs rpcbind about its program number, protocol, versions number(s) and port number(s).

Example of mountd program information generated via the rpcinfo command on a HP-UX server.

```
/usr/sbin/rpcinfo -p |grep mountd
   program vers proto   port  service
   100005    1   udp  49175  mountd
   100005    3   udp  49175  mountd
   100005    1   tcp  49207  mountd
   100005    3   tcp  49207  mountd
```

What does mountd do when it receives a mount request?

It does a "reverse lookup" of the IP address of the NFS client and hostname to validate the IP address and hostname so that it can compare that data to the access control lists. Next mountd gets the file handle of the requested NFS filesystem. With this information mountd can attempt to validate the client based on the access control and the entries in the /etc/xtab file. If the client is validated then mountd returns a file handle to the NFS client and adds an entry to the /etc/rmtab file.

After successful completion of these tasks the mountd program is no longer involved in the NFS transactions until the point that it receives a umount request. At that time it will remove the entry from the /etc/rmtab file.

Addressing Permission Denied Messages

The HP-UX NFS administration manuals have excellent guidelines for troubleshooting the common issues with NFS mount problems.

Please access the HP technical documentation site “I/O Cards and Networking Software” and review the troubleshooting sections of the relevant HP NFS manuals.

Click here to go to the main page for the HP technical documentation at:
http://www.docs.hp.com/en/netcom.html

Below are some example Scenarios of Permission Denied problems, along with how to gather advanced mountd debug.

Scenario One

The NFS server has an access list configured and has not granted the NFS client hostname access.

Mounting from the NFS client abox.atl.hp.com to the NFS server nfs-server.hp.com

abox# mount nfs-server:/nfsexport /nfsmount
Permission denied

From the NFS client, check the export options for the filesystem that are being trying to mount.

abox# showmount -e nfs-server
export list for nfs-server:
/nfsexport hosta.hp.com  <--------No hostname access for abox.atl.hp.com

If having access, always double check the exportfs output on the NFS server, the showmount results do not always display the full list of export options.

On the NFS-Server
nfs-server# exportfs
/nfsexport -access=hosta.hp.com<---Verified no access for abox.atl.hp.com

Fix the export options on the NFS server and re-export the filesystem.

Scenario Two

The NFS server has an access list and has granted the NFS client access to the NFS mount, but the format of the hostname in the export list does not match the results of the hostname lookup.

Mount from the NFS client abox.atl.hp.com to the NFS server nfs-server.hp.com

abox# mount nfs-server:/nfsexport /nfsmount
Permission denied

From the NFS client, check the export options

abox# showmount -e nfs-server
export list for nfs-server:
/nfsexport abox,hosta

From the NFS server, check the export options

nfs-server# exportfs -v
/nfsexport -access=abox:hosta

Here we see that the client hostname is in the access list. However, if we perform a lookup of the client IP & hostname on the NFS server we see that the hostname is resolved from the /etc/hosts file to the fully qualified name (FQDN).

nfs-server# nsquery hosts 16.113.145.126

Using "files" for the hosts policy.

Searching /etc/hosts for 16.113.145.126
Hostname: abox.atl.hp.com<----------Fully Qualified Hostname
Aliases:
Address: 16.113.145.126
Switch configuration: Terminates Search

nfs-server# nsquery hosts abox.atl.hp.com

Using "files" for the hosts policy.

Searching /etc/hosts for abox.atl.hp.com
Hostname: abox.atl.hp.com
Aliases:
Address: 16.113.145.126
Switch configuration: Terminates Search

If we query for the short name "abox" no results are returned.

nfs-server# nsquery hosts abox
Using "files" for the hosts policy.

Searching /etc/hosts for abox
abox was NOTFOUND
Switch configuration: Allows fallback
All name services have been searched

This is a common issue. The man page for exportfs states the following.

hostname
The name of a host. With a server configured for DNS naming in the nsswitch "hosts" entry, any hostname must be represented as a fully qualified DNS name. Currently HP-UX will allow a match for a non-fully qualified hostname; this HP only feature will be obsoleted in a later release of HP-UX.

The resolution is to match your exportfs options to the results of your name lookup queries. As can be seen the man page states at this point mountd will allow a match for a non-fully qualified hostname but be warned this feature will be obsoleted in later releases. It is best to configure the fully qualified name in the access list when specifying hostsnames.
Scenario Three

The hostname resolution and the exportfs options have already been checked and the problems are still there. The best thing to do is enable mountd debug and capture the failure.

Here is an example of the failure recorded in the mountd.log from scenario two.

Recap:
NFS Client hostname = abox.atl.hp.com
NFS server export options specify the shortname abox
NFS serer uses the /etc/hosts file for name resolution

Client receives Permission denied.

Steps to Capture Debug.

On the NFS server you can toggle debug on for the mountd program with the SIGUSR2 signal (kill -17) to the Process ID of the /usr/sbin/rpc.mountd program. The debug will be logged to the /var/adm/mountd.log.

Since a lot of data is logged when debug is enabled , toggle debug off again with another SIGUSR2 signal (kill -17) after reproducing the problem.

Example /var/adm/mountd.log

NOTE: We have removed several lines of debug in this example.

** Toggle Trace on **

< stuff deleted >

Here is the mount request from abox.atl.hp.com

03.02 11:26:45  nfs-server  pid=11275  rpc.mountd
rpc.mountd: mount: mount request from abox.atl.hp.com, mounting /nfsexport.
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
mountd: mount request from abox.atl.hp.com, mounting /nfsexport.

< stuff deleted>

Here we see that mountd checks the access list and notes that

it is not "null"

03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: in_access_list: access list = abox:hosta <---Here
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: in_access_list: restrictp is not NULL  <----Here

< stuff deleted>

Then mountd compares the hostname from the access list and the results of the name lookup on the target host.

03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: compare_hostnames_hp: sourcehost = 'abox'
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: compare_hostnames_hp: targethost = 'abox.atl.hp.com'
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd

03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: compare_hostnames_hp: return cannot determine -- namecomparison ambiguous

< stuff deleted>

Since mountd can not find a match, a permission denied message is sent back to the NFS client.

03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: mount: restricted access, not in access list
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
rpc.mountd: mount: mount request from abox.atl.hp.com denied: Permission denied
03.02 11:26:45  nfs-server   pid=11275  rpc.mountd
    mountd: mount request from abox.atl.hp.com denied: Permission denied

** Toggle Trace off **

TIP: As noted there will be a lot of debug logged to the /var/adm/mountd.log. Try searching on the Permission denied message and working your way back up the log file.

HP REFERENCES:

For HP NFS documentation visit HP's Technical documentation "I/O Cards and Networking Software" site.

Please click here for the latest documentation on the HP Technical site at:
http://www.docs.hp.com/en/netcom.html

Recommended HP documentation:

NFS Services Administrator's Guide

Managing NFS and KRPC Kernel Configurations in HP-UX 11i v2

NFS Performance Tuning for HP-UX v 11.0 and v 11i Systems

Books:

Title: Optimizing NFS Performance: Tuning and Troubleshooting NFS on HP-UX Systems
ISBN: 0130428167

## NFS: What are the NFS mount timeouts?

PROBLEM

When a NFS client is accessing a NFS server at mount time using the background option how long does it take for the mount command to timeout when the NFS server is offline?

When a NFS server is down the timeout issues are with the RPC calls to the NFS server sides portmapper/rpcbind
program. The client makes RPC GETPORT procedure calls to the NFS server sides portmapper program. You can set the NFS mount up with certain options to speed up the timeouts. Specifically the retry, background (bg) and version (vers) options.

HP-UX users will experience these delays when they are using the /etc/fstab to mount, any automounter maps
or from the command line.

See man mount_nfs for all options and descriptions.

RESOLUTION

Here is an example of a NFS client mount call and a network trace. In the trace the client is timing out trying to get the port for the mountd program from the portmapper daemon.

Mount command with out the background ( bg) option

1. Mount w/ out bg option:

```
# timex mount -o soft nfs_server:/tmp/hp /nfsmount
nfs mount: get_fh: nfs_server:: RPC: Rpcbind failure - RPC: Timed out
nfs mount: get_fh: nfs_server:: RPC: Rpcbind failure - RPC: Timed out
nfs mount: retry: retrying(1) for: /nfsmount after 5 seconds
nfs mount: retry: giving up on: /nfsmount
real     7:35.02
user        0.01
sys         0.01
```

2. Soft Mount w/ the bg option:

# timex mount -o soft,bg nfs_server:/tmp/hp /nfsmount
nfs mount: get_fh: nfs_server:: RPC: Rpcbind failure - RPC: Timed out
nfs mount: retry: retrying(1) for: /nfsmount after 5 seconds
nfs mount: retry: giving up on: /nfsmount
nfs mount: get_fh: nfs_server:: RPC: Rpcbind failure - RPC: Timed out
nfs mount: retry: backgrounding: /nfsmount
mount: Unable to update mnttab
real 3:45.02
user 0.01
sys 0.01

Here is a network trace of the event:
NETWORK TRACE:
No. Time Source Destination Protocol Info
672 13:51:20.002549 16.113.145.94 16.113.145.143 Portmap
V2 GETPORT Call
15 seconds

708 13:51:35.000127 16.113.145.94 16.113.145.143 Portmap
[RPC retransmission of #672]V2 GETPORT Call
30 seconds

738 13:52:05.000130 16.113.145.94 16.113.145.143 Portmap
[RPC retransmission of #672]V2 GETPORT Call
30 seconds

758 13:52:35.002963 16.113.145.94 16.113.145.143 Portmap
V2 GETPORT Call
30 seconds

764 13:52:50.000116 16.113.145.94 16.113.145.143 Portmap
[RPC retransmission of #758]V2 GETPORT Call
15 seconds

779 13:53:20.000128 16.113.145.94 16.113.145.143 Portmap

[RPC retransmission of #758]V2 GETPORT Call
30 seconds

824 13:53:50.001187 16.113.145.94 16.113.145.143 Portmap
V2 GETPORT Call
30 seconds

853 13:54:05.000119 16.113.145.94 16.113.145.143 Portmap
[RPC retransmission of #824]V2 GETPORT Call
30 seconds
905 13:54:35.000118 16.113.145.94 16.113.145.143 Portmap
[RPC retransmission of #824]V2 GETPORT Call
30 seconds

To decrease this time considerably you can specify the version of NFS you want to mount. This will reduce the
amount of portmapper calls.

With out specifying the version option the NFS client tries version 2 first then version 3.

Here is an example.

```
#timex mount -o bg,vers=3 gator:/tmp/hp /nfsmount
nfs mount: get_fh: gator:: RPC: Rpcbind failure - RPC: Timed out
nfs mount: retry: backgrounding: /nfsmount
real     1:15.03
user        0.01
sys         0.02
```

You can verify what version you are using with the nfsstat -m command on the HP-UX system.

You can test to see what versions your NFS server supports w/ the rpcinfo -p server_name command.

```
#rpcinfo -p nfs_server |grep -i nfs
   100003    2   tcp   2049  nfs
   100003    3   tcp   2049  nfs
   100003    2   udp   2049  nfs
   100003    3   udp   2049  nfs
#
```

## HP-UX NFS - What Are the New NFS Features that Are in v 11.31?

QUERY

Please provide a short summary of the new or changed features in HP-UX 11.31 for Network File System (NFS)

DETAILS

Here are a list of major changes, from the perspective of users of earlier HP-UX releases. For example, v 11.11 and v 11.23:

First, there are New NFS Configuration Files in addition to /etc/rc.config.d/nfsconf which are located in /etc/default as follows:

/etc/default/autofs - parameters for autofs which can be augmented in the nfsconf file.

/etc/default/nfs - The default NFS Version used by the Operating System(OS) is defined in addition to several other parameters not found in nfsconf. Take note that although 11.31 provides NFS v 4, the default version is v 3.

/etc/default/nfslogd - used to configure the new NFS server logging function used by all versions of NFS.

The second major change is that the exportfs command becomes a shell script and is functionally replaced by the "share" and "unshare" commands. man share(1M) for more info.

The third major change is that the /etc/exports file has been replaced by the /etc/dfs/dfstab file, and the format of the file has changed. man dfstab(4) for more info.

NOTE: NFS mounts at boot time continue to be specified in the /etc/fstab file.

NOTE: The remainder of the information in this article is paraphrased and/or summarized from the

following resource:

The "NFS Services Administrator's Guide: HP-UX 11i version 3" has more complete and up-to-date information on the new NFS features in HP-UX 11.31. Look for the guide on the main page.

Here is a list of the completely new NFS features in HP-UX 11.31:

Version 4 Protocol (NFSv4)

NFSv4 is an IETF standard protocol defined in RFC 3530. More information is available in the NFS Services Admin Guide.

Mount and umount enhancements

Starting with HP-UX 11i v3, the mount command is enhanced to provide benefits such as performance improvement of large sequential data transfers and local locking for faster access. The umount command allows forcible unmounting of filesystems. These features can be accessed using specific options of the mount command. For more information on these options, see mount_nfs (1M), and umount(1M).

Support for WebNFS

NFS is designed as a file access protocol for LANs. WebNFS is an extension of NFS. It enables you to access files across the Internet easily. WebNFS is designed to handle unique problems associated with accessing files across the Internet.

WebNFS enables filesystems at other locations on the Internet to appear to a user as a local filesystem. WebNFS works through firewalls and implements features such as read-ahead and write-behind, to improve throughput and performance over the Internet.

WebNFS is supported on NFS version 2 and 3 only.

Secure Sharing and mounting of Directories ("Secure NFS")

In earlier versions of HP-UX, NFS used the AUTH_SYS authentication, which uses UNIX style authentication, (uid/gid), to allow access to the shared files. It is fairly simple to develop an application or server that can masquerade as a user because the gid/uid ownership of a file can be viewed.

The AUTH_DH authenticating method was introduced to address the vulnerabilities of the AUTH_SYS authentication method. The AUTH_DH security model is stronger, because it authenticates the user by using the user’s private key.

Kerberos support has been added to provide authentication and encryption capabilities. Kerberos is an authentication system that provides secure transactions over networks. It offers strong user authentication, integrity and privacy.

Client Failover

By using client-side failover, an NFS client can specify redundant servers that are making the same data available and switch to an alternate server when the current server becomes unavailable. The filesystems on the current server can become unavailable for the following reasons:

If the filesystem is connected to a server that crashes

If the server is overloaded

If a network fault occurs

A failover occurs when the filesystem is unavailable. The failover is transparent to the user. The failover can occur at any time without disrupting processes that are running on the client.

Consider the following points before enabling client-side failover:

The filesystem must be mounted with read-only permissions.

The filesystems must be identical on all the redundant servers for the failover to occur successfully.

Enhanced NFS Logging

The NFS server logging enables an NFS server to provide a record of file operations that are performed on its filesystems. The record includes information about the file accessed, time of access, and the users who accessed the files. You can also specify the location of the logs that contain this information. This feature is useful for sites that make anonymous FTP archives available to NFS and WebNFS clients.

IPv6 Support

NFS supports filesystem mounting over an IPv4 or an IPv6 address where square brackets enclose the IPv6 address.

The nsquery feature supports ipnodes lookup request and provides support to lookup IPv6 data in the backend libraries.

## Book Reviews

Steve Woltering has written a review of "Time Management for System Administrators". Please click on: http://www.stats.ox.ac.uk/people/support_staff/saw/oreilly_reviews

## Security Bulletins – with thanks to Mike Ellison

## HP Security Bulletins – HP-UX

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00958338**

Version: 7

HPSBUX00246 SSRT3469 rev.7 - HP-UX sendmail, Remote Unauthorized Access, Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2003-03-03

Last Updated: 2007-08-21

Potential Security Impact: Remote unauthorized access, Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running sendmail, where the vulnerability may be exploited remotely to gain unauthorized access and create a Denial of Service

(DoS).

References: CERT CA-2003-07, CAN-2002-1337

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.10.10, B.10.20, B.11.00, B.11.04, B.11.11, and B.11.22

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.22
==========
InternetSrvcs.INETSVCS2-RUN
InternetSrvcs.INETSVCS-RUN
action: install PHNE_28409 or subsequent, modify /etc/mail/sendmail.cf

HP-UX B.11.11
==========
SMAIL-811.INETSVCS-SMAIL
action: install revision B.11.11.01.005 or subsequent, modify /etc/mail/sendmail.cf

InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35484 or subsequent

HP-UX B.11.04
==========
InternetSrvcs.INETSVCS-RUN
action: install PHNE_29526 or subsequent

HP-UX B.11.00
==========
SMAIL-811.INETSVCS-SMAIL
action: install B.11.00.01.004 or subsequent, modify /etc/mail/sendmail.cf

InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35483 or subsequent

HP-UX B.10.20
==========
InternetSrvcs.INETSVCS-RUN
action: PHNE_28760 or subsequent, modify /etc/mail/sendmail.cf

HP-UX B.10.10
==========
InternetSrvcs.INETSVCS-RUN
action: write to security-alert@hp.com for information

END AFFECTED VERSIONS

RESOLUTION
HP has made patches or web upgrades available to resolve the vulnerability.

The software patches are available on http://itrc.hp.com

The web upgrades are available from: http://www.hp.com/go/softwaredepot/

To resolve the vulnerability:

1. Determine the sendmail version:

Login in as root:
cd /usr/sbin
sendmail -d0.1 < /dev/null | grep -I version
The display will show Version #.#.#

2. Modify sendmail.cf if necessary

->B.11.22 sendmail 8.11.1,
->B.11.11: sendmail 8.11.1,
->B.11.00: sendmail 8.11.1,
->B.10.20 sendmail 8.9.3
modify /etc/mail/sendmail.cf as follows:

Add "restrictqrun" to the PrivacyOptions.
After the change the line should read:

O PrivacyOptions=authwarnings,restrictqrun

3. Install the appropriate patch or web upgrade

For HP-UX B.11.00 and B.11.11 sendmail 8.11.1
A web upgrade is available from: http://www.hp.com/go/softwaredepot/

The following software patches are available on http://itrc.hp.com

B.11.22 sendmail 8.11.1 PHNE_28409 or subsequent, modify /etc/mail/sendmail.cf
B.11.11 sendmail 8.9.3 ->PHNE_35484 or subsequent
B.11.04 sendmail 8.9.3 PHNE_29526 or subsequent
B.11.00 sendmail 8.9.3 ->PHNE_35483 or subsequent
B.10.20 sendmail 8.9.3 PHNE_28760 or subsequent, modify /etc/mail/sendmail.cf
B.10.10 Write to security-alert@hp.com for information

NOTE: If either of the following messages is received after applying the upgrade, please follow the recommended action.

warning: /etc/mail/aliases has world read or write permission. This is unsafe.
warning: /etc/mail/aliases.db has world read or write permission. This is unsafe.

Recommended action

Execute the following commands:

chmod 640 /etc/mail/aliases
chmod 640 /etc/mail/aliases.db
sendmail -bi

MANUAL ACTIONS: Yes - NonUpdate
->B.11.22 sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.11.11: sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.11.00: sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.10.20 sendmail 8.9.3: modify /etc/mail/sendmail.cf
B.10.10: write to security-alert@hp.com for information

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY

Revision: 0 (rev.0) - 03 March 2003 Initial release

Revision: 1 (rev.1) - Added information on upgrading from 8.8.6 to 8.9.3 or 8.11.1. Added information on warning messages; CERT and CVE reference numbers.

Revision: 2 (rev.2) - Corrected typo. Added 11.04(VVOS) information; 8.7.x to list of affected versions.

Revision: 3 (rev.3) - Added HPSecurityBul246.depot information. Replaced sendmail.811.11.11 file with sendmail.811.11.11.r1. Renamed sendmail.886.10.01 to sendmail.886.10.10. Clarified installation instructions.

Revision: 4 (rev.4) - Added note about HPSBUX0304-253. The files are in the SB246 subdirectory on the ftp site

Version: 5 (rev.5) - Final patches and web upgrades available.

Version: 6 (rev.6) - 12 April 2007 Reformatted

Version: 7 (rev.7) - 21 August 2007 PHNE_35483, PHNE_35484 automate previous manual actions

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01035741

Version: 11

HPSBUX00281 SSRT3631 rev.11 - HP-UX sendmail, Remote Unauthorized Privileged Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-02-22

Last Updated: 2007-08-21

Potential Security Impact: Remote unauthorized privileged access.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running sendmail, where the vulnerability could be exploited remotely to gain unauthorized privileged access.

References: CERT/CC CA-2003-25, CAN-2003-0681

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00, B.11.04, B.11.11, B.11.22, B.11.23 running sendmail 8.9.3 and 8.11.1.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.00
==========
InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35483 or subsequent

HP-UX B.11.00
==========
SMAIL-811.INETSVCS-SMAIL
action: install revision B.11.00.01.005 or subsequent modify /etc/mail/sendmail.cf

HP-UX B.11.04
==========
InternetSrvcs.INETSVCS-RUN
InternetSrvcs.INET-ENG-A-MAN
action: install PHNE_30224 or subsequent modify /etc/mail/sendmail.cf

HP-UX B.11.11
==========
InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35484 or subsequent

SMAIL-811.INETSVCS-SMAIL
action: install revision B.11.11.01.006 or subsequent modify /etc/mail/sendmail.cf

HP-UX B.11.22
==========
InternetSrvcs.INETSVCS2-RUN
InternetSrvcs.INETSVCS-RUN
action: install PHNE_29912 or subsequent modify /etc/mail/sendmail.cf

HP-UX B.11.23
==========
InternetSrvcs.INETSVCS2-RUN
->action: install PHNE_35485 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches and updates available to resolve the vulnerability.

The updates are available on http://itrc.hp.com

The updates are available on http://www.hp.com/go/softwaredepot/

B.11.00 Sendmail 8.9.3 ->PHNE_35483 or subsequent

B.11.00 Sendmail 8.11.1 B.11.00.01.005 or subsequent
B.11.04 Sendmail 8.9.3 PHNE_30224 or subsequent
B.11.11 Sendmail 8.9.3 ->PHNE_35484 or subsequent
B.11.11 Sendmail 8.11.1 B.11.11.01.006 or subsequent
B.11.22 Sendmail 8.11.1 PHNE_29912 or subsequent
B.11.23 Sendmail 8.11.1 ->PHNE_35485 or subsequent

Modify sendmail.cf if necessary

->B.11.22 sendmail 8.11.1,
->B.11.11: sendmail 8.11.1,
->B.11.00: sendmail 8.11.1,
->B.10.20 sendmail 8.9.3
modify /etc/mail/sendmail.cf as follows:

Add "restrictqrun" to the PrivacyOptions.
After the change the line should read:

O PrivacyOptions=authwarnings,restrictqrun

NOTE: HPSecurityBul281b should be removed before installing the patch or web upgrade if it had been installed::
swremove HPSecurityBul281b.INETSVCS-RUN

NOTE: If either of the following messages is received after applying the upgrade, please follow the recommended action.

warning: /etc/mail/aliases has world read or write permission. This is unsafe.
warning: /etc/mail/aliases.db has world read or write permission. This is unsafe.

Recommended action
Execute the following commands:
chmod 640 /etc/mail/aliases
chmod 640 /etc/mail/aliases.db
sendmail -bi

MANUAL ACTIONS: Yes - NonUpdate
->B.11.22 sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.11.11: sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.11.00: sendmail 8.11.1: modify /etc/mail/sendmail.cf
->B.10.20 sendmail 8.9.3: modify /etc/mail/sendmail.cf
B.10.10: write to security-alert@hp.com for information

PRODUCT SPECIFIC INFORMATION
HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY

Revision: 0 (rev.0) - 21 September 2003 Initial release
Revision: 1 (rev.1) - Added CAN-2003-0681
Revision: 2 (rev.2) - sendmail.811.11.22.r5 replaces sendmail.811.11.22.r4

Revision: 3 (rev.3) - HPSecurityBul281.depot available
Revision: 4 (rev.4) - HPSecurityBul281a.depot available
Revision: 5 (rev.5) - HPSecurityBul281b.depot adds B.11.23 and corrects B.11.22
Revision: 6 (rev.6) - Added PHNE_29773 and PHNE_29774; added Sendmail 8.11.1 B.11.00.01.005
Revision: 7 (rev.7) - Added PHNE_29912 and PHNE_29913
Revision: 8 (rev.8) - Added PHNE_30224
Revision: 9 (rev.9) - Added PHNE_31734
Version: 10 (rev.10) - 26 April 2007 Reformatted
Version: 11 (rev.11) - 21 August 2007 PHNE_35483, PHNE_35484, PHNE_35485 automate previous manual actions

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00571568

Version: 11

HPSBUX01137 SSRT5954 rev.11 - HP-UX Running TCP/IP (IPv4), Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-04-24

Last Updated: 2007-10-03

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running TCP/IP (IPv4). This vulnerability could be remotely exploited to cause a Denial of Service (DoS).

References: CAN-2005-1192

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.22, B.11.23 running TCP/IP (IPv4)

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems, verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
==========
Networking.NET2-KRN
action: install PHNE_33159 or subsequent

HP-UX B.11.22
==========
Networking.NET2-KRN
action: install preliminary binary files per Security Bulletin HPSBUX01164

HP-UX B.11.23
==========
Networking.NET2-KRN
action: install PHNE_32606 or subsequent

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN
->action: install IPSec revision A.02.01.01 or subsequent and PHNE_35351 or subsequent

HP-UX B.11.23
==========
IPSec.IPSEC2-KRN
->action: install IPSec revision A.02.01.01 or subsequent and PHNE_35766 or subsequent

END AFFECTED VERSIONS

Certain network traffic can result in a Denial of Service (DoS) for HP-UX systems running TCP/IP (IPv4). Receiving a certain packet on any open TCP/IP connection can result in a Denial of Service (DoS) condition which can only be corrected by a reboot of the affected system. The Denial of Service (DoS) is characterized by high cpu utilization and a lack of response on any I/O port including the system console.

Previous revisions of this Security Bulletin recommended setting ip_pmtu_strategy to 0 or 3 as a workaround. Patches or updates to resolve the issue are now available. After these patches or updates are installed the workaround will no longer be necessary or recommended.

The ip_pmtu_strategy parameter should be restored to the default value of 1.
Note: Previous versions of this Security Bulletin incorrectly stated that the default value of ip_pmtu_strategy is 2.

RESOLUTION
To resolve the vulnerability HP has provided patches and updates.

Patches are available from http://itrc.hp.com

Updates are available from http://www.hp.com/go/softwaredepot

HP-UX B.11.11 without IPSec install PHNE_33159 or subsequent
HP-UX B.11.11 with IPSec ->install IPSec revision A.02.01.01 or subsequent and PHNE_35351 or subsequent
HP-UX B.11.23 without IPSec install PHNE_32606 or subsequent
HP-UX B.11.23 with IPSec ->install IPSec revision A.02.01.01 or subsequent and PHNE_35766 or subsequent

For HP-UX B.11.22, install preliminary binary files per Security Bulletin HPSBUX01164.

MANUAL ACTIONS: Yes - NonUpdate
HP-UX B.11.22 Install preliminary binary files per Security Bulletin HPSBUX01164.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY

Revision 0 (rev.0) - 24 April 2005 Initial release
Revision 1 (rev.1) - 25 May 2005 Binary files available per Security Bulletin HPSBUX01164
Revision 2 (rev.2) - 1 June 2005 IPSec not included in binary files
Revision 3 (rev.3) - 27 June 2005 PHNE_33159 is available for B.11.11
Revision 4 (rev.4) - 10 July 2005 PHNE_32606 is available for B.11.23
Revision 5 (rev.5) - 24 July 2005 Clarified the Resolution and Manual Actions sections
Revision 6 (rev.6) - 5 December 2005 IPSec revisions available
Version 7 (rev.7) - Skipped for formatting reasons
Version 8 (rev.8) - 23 January 2006 Add rev. to title
Version 9 (rev.9) - 2 April 2007 Change A.2.00.01 to A.02.00.01
Version 10 (rev.10) - 30 April 2007 Default value for ip_pmtu_strategy is 1, not 2
Version 11 (rev.11) - 3 October 2007 IPSec revision A.02.01.01 available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00572922

Version: 2

HPSBUX02079 SSRT5957 rev.2 - HP-UX IPSec Encapsulating Security Payload (ESP) Tunnel Mode, Remote Unauthorized Disclosure of Encrypted Data

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-12-01

Last Updated: 2007-08-08

Potential Security Impact: Remote unauthorized disclosure of encrypted data

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified for HP-UX running IPSec using Encapsulating Security Payload (ESP) in Tunnel Mode without authentication. These vulnerabilities could be exploited by a remote unauthorized user to intercept a portion of the plain-text message.

References: NISCC VU#004033, CAN-2005-0039

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00, B.11.11, B.11.23 running IPSec

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.23
HP-UX B.11.11
HP-UX B.11.00
==========
IPSec.IPSEC2-KRN
action: configure ESP to use both encryption and authentication

END AFFECTED VERSIONS

RESOLUTION
The recommended resolution is to configure ESP to use both encryption and authentication. "ECP-DES", ECP-3DES", and "ECP-AES128" provide only encryption and should not be used.

For more information please refer to /usr/share/doc/ipsec.pdf.

Note: In HP-UX IPSec version A.2.01 the ipsec_config command no longer allows the configuration of transforms for ESP without authentication. Existing policies that use such transforms will continue to work. However, these
should be replaced with ESP transforms that provide both encryption and authentication. Please refer to the HP-UX IPSec version A.2.01 Release Notes for further information.

MANUAL ACTIONS: Yes – NonUpdate -Configure ESP to use both encryption and authentication.

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=B6834AA

UPDATE HISTORY

Version:1 (rev.1) - 05 December 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00555601

Version: 2

HPSBUX02076 SSRT5979 rev.2 - HP-UX Running IPSec, Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-11-11

Last Updated: 2007-08-08

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential vulnerabilities have been identified with HP-UX running IPSec.

These vulnerabilities may be exploited remotely by an unauthorized user to create a Denial of Service (DoS).

References: NISCC Vulnerability Advisory 273756

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00, B.11.11, and B.11.23 running IPSec.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.00
==========
IPSec.IPSEC2-KRN
action: install revision A.01.05.01 or subsequent

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN
action: install revision A.01.07.02 or subsequent

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN,revision=A.02.00
action: install revision A.02.01 or subsequent

HP-UX B.11.23
==========
IPSec.IPSEC2-KRN
action: install revision A.02.01 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following software updates available to resolve the issue.
The updates are available from http://www.hp.com/go/softwaredepot

HP-UX B.11.00 HP-UX IPSec A.01.05.01 or subsequent
HP-UX B.11.11 HP-UX IPSec A.01.07.02

HP-UX B.11.11 HP-UX IPSec A.02.01 or subsequent
HP-UX B.11.23 HP-UX IPSec A.02.01 or subsequent

MANUAL ACTIONS: Yes - Update

HP-UX B.11.00 HP-UX IPSec A.01.05.01 or subsequent
HP-UX B.11.11 HP-UX IPSec A.01.07.02
HP-UX B.11.11 HP-UX IPSec A.02.01 or subsequent
HP-UX B.11.23 HP-UX IPSec A.02.01 or subsequent

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/display ProductInfo.pl?productnumber=B6834AAtN

UPDATE HISTORY
Version:1 (rev.1) - 15 November 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00547561

Version: 2

HPSBUX02073 SSRT051012 rev.2 - HP-UX envd, Local Execution of Privileged Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-11-08

Last Updated: 2007-08-08

Potential Security Impact: Local execution of privileged code.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential vulnerability has been identified with HP-UX running the envd(1M). The vulnerability could be exploited by a local authorized user to execute arbitrary code and/or gain unauthorized privileges.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00 and B.11.11.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.00
==========
OS-Core.UX-CORE
action: install PHCO_33989 or subsequent

HP-UX B.11.11
==========
OS-Core.UX-CORE
action: install PHCO_33967 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve this issue.
The patches are downloadable from: http://itrc.hp.com

HP-UX B.11.00 PHCO_33989 or subsequent
HP-UX B.11.11 PHCO_33967 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION
HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

UPDATE HISTORY
Version:1 (rev.1) - 08 November 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

MANUAL ACTIONS - No

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00574124

Version: 2

HPSBUX02082 SSRT051037 rev.2 - HP-UX Running IPSec, Remote Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-12-01

Last Updated: 2007-08-08

Potential Security Impact: Remote unauthorized access

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been discovered with HP-UX running IPSec. The vulnerability could be exploited to allow remote unauthorized access.

References: None.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00, B.11.11, and B.11.23 running IPSec.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.00
==========
IPSec.IPSEC2-KRN
action: install revision A.01.05.01 or subsequent

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN
action: install revision A.01.07.02 or subsequent

HP-UX B.11.23
==========
IPSec.IPSEC2-KRN
action: install revision A.02.01 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following software updates available to resolve the issue. The updates are available from http://www.hp.com/go/softwaredepot

HP-UX B.11.00 HP-UX IPSec A.01.05.01 or subsequent
HP-UX B.11.11 HP-UX IPSec A.01.07.02 or subsequent
HP-UX B.11.23 HP-UX IPSec A.02.01 or subsequent

MANUAL ACTIONS: Yes - Update
HP-UX B.11.00 update to HP-UX IPSec A.01.05.01 or subsequent
HP-UX B.11.11 update to HP-UX IPSec A.01.07.02 or subsequent
HP-UX B.11.23 update to HP-UX IPSec A.02.01 or subsequent

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=B6834AA

UPDATE HISTORY
Version:1 (rev.1) - 05 December 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00629555

Version: 15

HPSBUX02108 SSRT061133 rev.15 - HP-UX Running sendmail, Remote Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-08-08

Last Updated: 2007-08-21

Potential Security Impact: Remote execution of arbitrary code

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A vulnerability has been identified in sendmail which may allow a remote attacker to execute arbitrary code.

References: CVE-2006-0058, US-CERT VU#834865

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.23 running sendmail 8.13.3, sendmail 8.11.1 HP-UX B.11.11 running sendmail 8.13.3, sendmail 8.11.1, sendmail 8.9.3 HP-UX B.11.04 running sendmail 8.9.3 HP-UX B.11.00 running sendmail 8.11.1, sendmail 8.9.3, sendmail 8.8.6

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

For sendmail 8.13.3
HP-UX B.11.23
==========
SMAIL-UPGRADE.INET-SMAIL
SMAIL-UPGRADE.INET2-SMAIL
action: install revision B.11.23.01.003 or subsequent, modify /etc/mail/sendmail.cf to add 'restrictqrun' to the PrivacyOptions.
URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=SMAIL813

HP-UX B.11.11
==========
SMAIL-UPGRADE.INETSVCS-SMAIL

action: install revision B.11.11.02.004 or subsequent, modify /etc/mail/sendmail.cf to add 'restrictqrun' to the PrivacyOptions.
URL:
http://h20293.www2.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=SMAIL813

For sendmail 8.11.1
HP-UX B.11.23
==========
UNOF_INET31734_1.INETSVCS2-RUN
UNOF_INET31734_3.INETSVCS2-RUN
UNOF_INET31734_4.INETSVCS2-RUN
action: remove any unofficial patch if installed InternetSrvcs.INETSVCS2-RUN
->action: install PHNE_35485 or subsequent

HP-UX B.11.11
==========
SMAIL-811.INETSVCS-SMAIL
action: install revision B.11.11.01.010 or subsequent, modify /etc/mail/sendmail.cf to add 'restrictqrun' to the PrivacyOptions.
URL:
ftp://sendmail:sendmail@hprc.external.hp.com/
sendmail-811_10.depot

HP-UX B.11.00
==========
SMAIL-811.INETSVCS-SMAIL
action: install revision B.11.00.01.009 or subsequent, modify /etc/mail/sendmail.cf to add 'restrictqrun' to the PrivacyOptions.
URL:
http://h20293.www2.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=SMAIL811

For sendmail 8.9.3
HP-UX B.11.11
==========
UNOF_INET_29774_1.INETSVCS-RUN
UNOF_INET_29774_2.INETSVCS-RUN
UNOF_INET_29774_3.INETSVCS-RUN
action: remove any unofficial patch if installed InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35484 or subsequent

HP-UX B.11.00
==========
UNOF_INET_29773_1.INETSVCS-RUN
UNOF_INET_29773_2.INETSVCS-RUN
UNOF_INET_29773_3.INETSVCS-RUN
action: remove any unofficial patch if installed InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35483 or subsequent

HP-UX B.11.04
==========
UNOF_INET_29773_1.INETSVCS-RUN
UNOF_INET_29773_2.INETSVCS-RUN
UNOF_INET_29773_3.INETSVCS-RUN
action: remove any unofficial patch if installed InternetSrvcs.INETSVCS-RUN
action: install PHNE_34927 or subsequent

For sendmail 8.8.6
HP-UX B.11.00
==========
UNOF_INET_29773_1.INETSVCS-RUN
UNOF_INET_29773_2.INETSVCS-RUN
UNOF_INET_29773_3.INETSVCS-RUN
action: remove any unofficial patch if installed InternetSrvcs.INETSVCS-RUN
->action: install PHNE_35483 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has made the following software updates and patches available to resolve the issue.

The patches are available from http://itrc.hp.com while webupgrades can be downloaded from http://software.hp.com

The preliminary software updates can be downloaded via ftp from:

System: hprc.external.hp.com (192.170.19.100)
Login: sendmail
Password: sendmail (NOTE: CASE-sensitive)

ftp://sendmail:sendmail@hprc.external.hp.com

or

ftp://sendmail:sendmail@192.170.19.100

The webupgrades for sendmail 8.13.3 on B.11.11 as well as B.11.23 can be downloaded from http://software.hp.com using the URL above.

The cksum and md5 output for the preliminary depots are listed below.

The cksum and md5 output are also found the README.txt.pgp on the ftp site.

For sendmail 8.13.3, HP-UX B.11.23
sendmail -bs banner:
Sendmail version 8.13.3 - Revision 1.003 - 2006/05/24
what(1) string:
Sendmail version 8.13.3 - Revision 1.003 - 05/24/2006

For sendmail 8.13.3, HP-UX B.11.11
sendmail -bs banner:
Sendmail version 8.13.3 - Revision 2.004 - 2006/06/29
what(1) string:
Sendmail version 8.13.3 - Revision 2.004 - 06/29/2006

For sendmail 8.11.1, HP-UX B.11.23
Note: If UNOF_INET31734_1.depot or UNOF_INET31734_3.depot or UNOF_INET31734_4.depot has been installed, they must be removed using swremove(1M) before installing PHNE_35485 or subsequent.

For sendmail 8.11.1, HP-UX B.11.11

sendmail-811_10.depot
cksum 3720753575 2949120
md5 01f5e7c1a67c0b0a1103abdaa2907f21
sendmail -bs banner:
Sendmail 8.11.1 (Revision 1.10)
what(1) string:
version.c 8.11.1 (Berkeley) - (Revision 1.10) - 17th July 2006

For sendmail 8.11.1, HP-UX B.11.00
sendmail -bs banner:
Sendmail 8.11.1 - (Revision 1.09)
what(1) string:
version.c 8.11.1 (Berkeley) - (Revision 1.09) - 4th July 2006

For sendmail 8.9.3, HP-UX B.11.11
If UNOF_INET_29774_3.depot or previous is installed, remove it using swremove(1M).
Then install: ->PHNE_35484 or subsequent

For sendmail 8.9.3, HP-UX B.11.00
If UNOF_INET_29772_3.depot or previous is installed, remove it using swremove(1M).
Then install: ->PHNE_35483 or subsequent

For sendmail 8.9.3, HP-UX B.11.04
If UNOF_INET_29772_3.depot or previous is installed, remove it using swremove(1M).
Then install: PHNE_34927 or subsequent
sendmail -bs banner:
Sendmail 8.9.3 (PHNE_32006)/8.9.3; Fri, 7 Jul 2006
what(1) string:
version.c 8.9.3.1 (Berkeley) 11/05/2006 (PHNE_32006)
Special Installation Instructions - Note: sendmail is not supported in daemon mode on VVOS platforms. It is provided as a mailing agent (outbound) only.

For sendmail 8.8.6, HP-UX B.11.00
If UNOF_INET_29772_3.depot or previous is installed, remove it using swremove(1M).
Then install: ->PHNE_35484 or subsequent
->Note: PHNE_35484 or subsequent upgrades sendmail 8.8.6 to sendmail 8.9.3.

For all versions of sendmail:

->If PHNE_35483, PHNE_35484, PHNE_35485 or subsequent is not installed, modify sendmail.cf to add 'restrictqrun' to the PrivacyOptions.

After installation, verify output of what /usr/sbin/sendmail.
To check if installations are running sendmail 8.8.6 execute "what /usr/sbin/sendmail" and check the version string.

MANUAL ACTIONS: Yes - NonUpdate
->If PHNE_35483, PHNE_35484, PHNE_35485 or subsequent is not installed, modify /etc/mail/sendmail.cf to add 'restrictqrun' to the PrivacyOptions

HP-UX B.11.11 - install preliminary software
HP-UX B.11.23 - install preliminary software

PRODUCT SPECIFIC INFORMATION
HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=B6834AA

HISTORY:
Version: 1 (rev.1) - 25 March 2006 Initial release
Version: 2 (rev.2) - 30 March 2006 updated md5 / cksum output
Version: 3 (rev.3) - 04 April 2006 updated B.11.23 depot, added 8.11.1 for B.11.23 depot
Version: 4 (rev.4) - 07 April 2006 added 8.9.3 depot for B.11.11
Version: 5 (rev.5) - 10 April 2006 clarified affected versions
Version: 6 (rev.6) - 12 April 2006 added 8.9.3 and 8.11.1 depots for B.11.00
Version: 7 (rev.7) - 18 April 2006 added 8.11.1 upgrade for HP-UX B.11.11
Version: 8 (rev.8) - 24 April 2006 replaced 8.9.3 depot for HP-UX B.11.00 and B.11.11
Version: 9 (rev.9) - 25 April 2006 added manual actions
Version: 10 (rev.10) - 03 May 2006 replaced 8.9.3 depot for HP-UX B.11.00 and B.11.11, added 8.11.1 depot for B.11.00
Version: 11 (rev.11) - 18 May 2006 sendmail 8.11.1 replacements UNOF_INET31734_4, sendmail-811_01.008 depot, and sendmail-811_09.depot, sendmail 8.9.3 new PHNE_31917, sendmail 8.8.6, sendmail 8.9.3 new PHNE_32006
Version: 12 (rev.12) - 18 July 2006 added webupgrades for 8.11.1 on B.11.00, and 8.13.3 on B.11.11; added patch for B.11.04.
Version: 13 (rev.13) - 31 July 2006 added PHNE_34900 for 8.9.3 on B.11.00, PHNE_34936 for 8.9.3 on B.11.11, PHNE_34689 for 8.11.1 on B.11.23, sendmail-811_01.009, sendmail-811_10.depot.
Version: 14 (rev.14) - 08 August 2006 corrected typo on 8.11.1 on B.11.23,
Version: 15 (rev.15) 21 August 2007 PHNE_35483, PHNE_35484, PHNE_35485 automate previous manual actions

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00771742

Version: 6

HPSBUX02153 SSRT061181 rev.6 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-09-20

Last Updated: 2007-09-17

Potential Security Impact: Remote unauthorized access or elevation of privileges or Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified in Firefox running on HP-UX. These vulnerabilities could be exploited remotely resulting in unauthorized access, elevation of privileges, or Denial of Service (DoS).

References: Mozilla Foundation Security Advisory (MFSA) 2006-20, 2006-22 to 2006-25, 2006-27 to 2006-39, 2006-41 to 2006-48, 2006-50 to 2006-62, 2006-64 to 2006-73, 2006-75, 2006-76, 2007-01 to 2007-09, 2007-11 to 2007-27.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
->Firefox prior to v2.0.0.6 running on HP-UX B.11.11 and B.11.23.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

For further information please refer to:
http://www.mozilla.org/projects/security/known-vulnerabilities.html

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
==========
Firefox.FFOX-COM
->action: install revision 2.0.0.6 or subsequent
-> URL:
ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/2.0.0.6/contrib/

END AFFECTED VERSIONS

RESOLUTION
->Preliminary versions of Firefox v2.0.0.6 are available to resolve the potential vulnerabilities. These preliminary versions have received minimal testing and are localized for English only. The preliminary versions are available for download as above

For HP-UX B.11.23 (IA):
-> ffox_200600alpha_ia.depot
-> ffox_200600alpha_ia.depot.readme

For HP-UX B.11.11 and B.11.23 (PA):
-> ffox_200600alpha_pa.depot
-> ffox_200600alpha_pa.depot.readme

->This security bulletin will be revised when fully tested and localized versions of Firefox v2.0.0.6 or subsequent for HP-UX are available.

->The most recent fully tested and localized Firefox (v2.0.0.4) is available here:
http://www.hp.com/products1/unix/java/firefox/index.html

MANUAL ACTION: Yes - Update ->Install Firefox v2.0.0.6

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY
Version:1 (rev.1) - 20 September 2006 Initial release
Version:2 (rev.2) - 29 November 2006 preliminary Firefox v1.5.0.8 available
Version:3 (rev.3) - 27 February 2007 preliminary Firefox v1.5.0.9 available
Version:4 (rev.4) - 18 July 2007 preliminary Firefox v2.0.0.4 available

Version:5 (rev.5) - 22 August 2007 fully tested and localized Firefox v2.0.0.4 available
Version:6 (rev.6) - 17 September 2007 preliminary Firefox v2.0.0.6 available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00774579

Version: 3

HPSBUX02156 SSRT061236 rev.3 - HP-UX Running Thunderbird, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-09-20

Last Updated: 2007-08-27

Potential Security Impact: Remote unauthorized access, elevation of privileges, Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified in Thunderbird running on HP-UX. These vulnerabilities could be exploited remotely resulting in unauthorized access, elevation of privileges, or Denial of Service (DoS).

References: ->Mozilla Foundation Security Advisory (MFSA) 2006-74, 2006-73, 2006-72, 2006-71, 2006-70, 2006-69, 2006-68, 2006-67, 2006-66, 2006-65, 2006-64, 2006-63, 2006-60, 2006-59, 2006-58, 2006-57, 2006-55, 2006-54, 2006-53, 2006-52, 2006-51, 2006-50, 2006-49, 2006-48, 2006-47, 2006-46, 2006-44, 2006-42, 2006-40, 2006-38, 2006-37, 2006-35, 2006-33, 2006-32, 2006-31, 2006-28, 2006-27, 2006-26, 2006-25, 2006-24, 2006-22, 2006-21, 2006-20, 2006-08, 2006-07, 2006-06, 2006-05, 2006-04, 2006-02, 2006-01.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
->Thunderbird prior to version 1.5.0.9 running on HP-UX B.11.11, B.11.23, and B.11.31.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

For further information please refer to:
http://www.mozilla.org/projects/security/known-vulnerabilities.html

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
->HP-UX B.11.31
==========
Tbird.TBIRD-COM
action: install revision 1.5.0.9 or subsequent

URL:
ftp://ftp.mozilla.org/pub/mozilla.org/thunderbird/releases/1.5.0.9/contrib/

END AFFECTED VERSIONS

RESOLUTION
HP has made preliminary versions of Thunderbird 1.5.0.9 available to resolve the issue. These preliminary versions have received minimal testing and are localized for English only. The preliminary versions are available for download as above.

->For HP-UX B.11.23 and B.11.31 (IA):
thunderbird_1.5.0.9_ia.depot.gz
thunderbird_1.5.0.9_ia.depot.gz.readme

->For HP-UX B.11.11, B.11.23, and B.11.31 (PA):
thunderbird_1.5.0.9_pa.depot.gz
thunderbird_1.5.0.9_pa.depot.gz.readme

This security bulletin will be revised when fully tested and localized versions of Thunderbird 1.5.0.9 or subsequent for HP-UX are available.

The most recent fully tested and localized Thunderbird (version 1.5.0.8) is available here:
http://www.hp.com/products1/unix/java/firefox/index.html

Thunderbird version 1.5.0.8 does not resolve the following: Mozilla Foundation Security Advisory (MFSA) 2006-74, 2006-73, 2006-72, 2006-71, 2006-70, 2006-69, 2006-68. These are resolved in Thunderbird version 1.5.0.9.

MANUAL ACTION: Yes – Update - install revision 1.5.0.9 or subsequent

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY
Version:1 (rev.1) - 20 September 2006 Initial release
Version:2 (rev.2) - 05 March 2007 preliminary Thunderbird 1.5.0.9 available
Version:3 (rev.3) - 27 August 2007 added HP-UX B.11.31

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00837319

Version: 3

HPSBUX02181 SSRT061289 rev.3 - HP-UX Running IPFilter, Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-16

Last Updated: 2007-10-03

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running IPFilter in combination with PHNE_34474. The vulnerability could be remotely exploited to create a Denial of Service (DoS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.23 running IPFilter with PHNE_34474 installed.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

A successful exploit will result in a system crash.

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems, verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.23
==========
IPF-HP.IPF-MIN
->action: install PHNE_35545 or subsequent and PHNE_35766 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve the vulnerability. The patches are available from http://itrc.hp.com

->PHNE_35545 or subsequent and PHNE_35766 or subsequent

->Note: If the preliminary patch UNOF_35938.depot has been installed, it
should be removed before installing PHNE_35545 or subsequent.

->Note: Previous versions of this Security Bulletin recommended disabling IPFilter. After installing the recommended patches, it is no longer necessary to disable IPFilter.

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY
Version:1 (rev.1) 16 January 2007 Initial release
Version:2 (rev.2) 5 February 2007 UNOF_35938.depot available
Version:3 (rev.3) 3 October 2007 PHNE_35545 and PHNE_35766 are available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01090656

Version: 1

HPSBUX02247 SSRT071432 rev.1 - HP-UX Running ARPA Transport, Local Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-07-25

Last Updated: 2007-07-25

Potential Security Impact: Local Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running ARPA Transport. The vulnerability could be exploited locally by an authorized user to create a Denial of Service (DoS).

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23 running ARPA Transport.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

AFFECTED VERSIONS

Note: To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

HP-UX B.11.11
==========
OS-Core.CORE2-KRN
action: install PHNE_35351 or subsequent

HP-UX B.11.23
==========
OS-Core.CORE2-KRN
action: install PHNE_35766 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following software patches available to resolve the vulnerability.
These patches are available on: http://itrc.hp.com

HP-UX B.11.11 PHNE_35351 or subsequent
HP-UX B.11.23 PHNE_35766 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 25 July 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01087206

Version: 1

HPSBUX02248 SSRT071437 rev.1 - HP-UX Running ARPA Transport, Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-07-25

Last Updated: 2007-07-25

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running ARPA Transport. The vulnerability could be exploited remotely to create a Denial of Service (DoS).

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running ARPA Transport.

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

AFFECTED VERSIONS

Note: To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

HP-UX B.11.11
==========
Networking.NET2-KRN
action: install PHNE_35351 or subsequent

HP-UX B.11.23
==========
Networking.NET2-KRN
action: install PHNE_35766 or subsequent

HP-UX B.11.31
==========
Networking.NET2-KRN
action: install PHNE_35352 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following software patches available to resolve the vulnerability.

These patches are available on: http://itrc.hp.com

HP-UX B.11.11 PHNE_35351 or subsequent
HP-UX B.11.23 PHNE_35766 or subsequent
HP-UX B.11.31 PHNE_35352 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 25 July 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01167886**

Version: 1

HPSBUX02259 SSRT071439 rev.1 - HP-UX Running logins(1M), Remote Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-09-18

Last Updated: 2007-09-18

Potential Security Impact: Remote unauthorized access.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in HP-UX running the logins(1M) command. This command incorrectly reports password status. As a result password issues may not be detected, allowing remote unauthorized access.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running logins(1M)

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The logins(1m) command incorrectly reports password status. As a result password issues may not be detected, allowing remote unauthorized access.

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
==========
SOE.SOE
action: install PHCO_36809 or subsequent

HP-UX B.11.23
==========
SOE.SOE
action: install PHCO_36808 or subsequent

HP-UX B.11.31
==========
SOE.SOE
action: install PHCO_36003 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve the issue.
The patches are available on: http://itrc.hp.com

B.11.11 PHCO_36809 or subsequent

B.11.23 PHCO_36808 or subsequent
B.11.31 PHCO_36003 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION
HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 18 September 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01118367

Version: 2

HPSBUX02249 SSRT071442 rev.2 - HP-UX Running the Ignite-UX or the DynRootDisk (DRD) get_system_info Command, Local Unqualified Configuration Change

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-20

Last Updated: 2007-09-12

Potential Security Impact: Local unqualified configuration change

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in HP-UX running the Ignite-UX or the DynRootDisk (DRD) get_system_info command. This command can change system networking parameters without notification.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running the Ignite-UX vC.7.0, vC.7.1, vC.7.2, vC.7.3 or the DynRootDisk (DRD) vA.1.0.16.417, vA.1.0.18.245, vA.1.1.0.344, vA.2.0.0.592 get_system_info command.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The get_system_info command is executed by the following commands:
make_net_recovery
make_tape_recovery

save_config
drd

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
==========
Ignite-UX.MGMT-TOOLS,revision=C.7.0.212
->Ignite-UX.MGMT-TOOLS,revision=C.7.1.93
->Ignite-UX.MGMT-TOOLS,revision=C.7.2.94
Ignite-UX.MGMT-TOOLS,revision=C.7.3.144
action: use the script from the Resolution to work around the vulnerability

HP-UX B.11.23
HP-UX B.11.31
==========
DRD.DRD-RUN,revision=A.1.0.16.417
DRD.DRD-RUN,revision=A.1.0.18.245
DRD.DRD-RUN,revision=A.1.1.0.344
DRD.DRD-RUN,revision=A.2.0.0.592
action: use the script from the Resolution to work around the vulnerability

END AFFECTED VERSIONS

RESOLUTION
Until an update is available, HP has made the following workaround procedure available to resolve the issue.

-> Note: The script has changed. The script recommended in rev.1 of this Security Bulletin did not correctly check the HP Ignite-UX revision number. The original script would only install itself on HP Ignite-UX revision C.7.3.144. The new script documented below will work properly on all vulnerable revisions of HP Ignite-UX. Either the old or new script will work correctly with DynRootDisk.

->The procedure below moves the get_system_info program to another directory and replaces it with a script. The script temporarily disables the autopush program, runs the original get_system_info, and then enables autopush. By running the original get_system_info program with antopush disabled the vulnerability is avoided. More details are documented in the script.

1. Download the script "get_system_info.wrapper" from the following ftp site:
ftp://ss071442:ss071442@hprc.external.hp.com/

2 .Verify the cksum or md5 sum:
->cksum: 2284708550 5344 get_system_info.wrapper
->MD5 (get_system_info.wrapper) = 6ed1dfc6508e2cb45f8624a8ed31611f

->The new script contains this line:
# @(#) $Date: 2007-09-11 10:30:49 -0600 (Tue, 11 Sep 2007) $ $Revision: 71524 $

3. As root, copy the script into a secure directory.

4. As root, run the script. The script will display the files it is replacing.

For example:

#$secure_directory/get_system_info.wrapper
Replacing /opt/ignite/lbin/get_system_info with $secure_directory/get_system_info.wrapper
Replacing /opt/drd/lbin/get_system_info with $secure_directory/get_system_info.wrapper

where $secure_directory is the path to the secure directory containing the script.

5. The script must be executed whenever a vulnerable version of the fileset Ignite-UX.MGMT-TOOLS or the fileset DRD.DRD-RUN is reinstalled.

MANUAL ACTIONS: Yes - NonUpdate
Use script in Resolution section to work around the vulnerability

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY
Version: 1 (rev.1) - 20 August 2007 Initial release
Version: 2 (rev.2) - 12 September 2007 new script, corrected revision numbers

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01178795

Version: 1

HPSBUX02262 SSRT071447 rev. 1 - HP-UX running Apache, Remote Arbitrary Code Execution, Cross Site Scripting (XSS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-10-02

Last Updated: 2007-10-02

Potential Security Impact: Remote arbitrary code execution, cross site scripting (XSS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with Apache running on HP-UX. The vulnerabilities could be exploited remotely via Cross Site Scripting (XSS) to execute arbitrary code.

References: CVE-2005-2090, CVE-2006-5752, CVE-2007-0450, CVE-2007-0774, CVE-2007-1355, CVE-2007-1358, CVE-2007-1860, CVE-2007-1863, CVE-2007-1887, CVE-2007-1900, CVE-2007-2449, CVE-2007-2450, CVE-2007-2756, CVE-2007-2872, CVE-2007-3382, CVE-2007-3385, CVE-2007-3386.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running Apache

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

For IPv4:
HP-UX B.11.11
==========
hpuxwsAPACHE
action: install revision A.2.0.59.00 or subsequent restart Apache
URL: https://www.hp.com/go/softwaredepot/

For IPv6:
HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
==========
hpuxwsAPACHE,revision=B.1.0.00.01
hpuxwsAPACHE,revision=B.1.0.07.01
hpuxwsAPACHE,revision=B.1.0.08.01
hpuxwsAPACHE,revision=B.1.0.09.01
hpuxwsAPACHE,revision=B.1.0.10.01
hpuxwsAPACHE,revision=B.2.0.48.00
hpuxwsAPACHE,revision=B.2.0.49.00
hpuxwsAPACHE,revision=B.2.0.50.00
hpuxwsAPACHE,revision=B.2.0.51.00
hpuxwsAPACHE,revision=B.2.0.52.00
hpuxwsAPACHE,revision=B.2.0.53.00
hpuxwsAPACHE,revision=B.2.0.54.00
hpuxwsAPACHE,revision=B.2.0.55.00
hpuxwsAPACHE,revision=B.2.0.56.00
hpuxwsAPACHE,revision=B.2.0.58.00
hpuxwsAPACHE,revision=B.2.0.58.01

action: install revision B.2.0.59.00 or subsequent restart Apache
URL: https://www.hp.com/go/softwaredepot/

END AFFECTED VERSIONS

RESOLUTION
HP has made the following available to resolve the vulnerability.
HP-UX Apache-based Web Server v.2.18 powered by Apache Tomcat Webmin or subsequent.

The update is available as above

Note: HP-UX Apache-based Web Server v.2.18 powered by Apache Tomcat Webmin contains HP-

UX Apache-based Web Server v.2.0.59.00.

MANUAL ACTIONS: Yes - Update
Install HP-UX Apache-based Web Server v.2.18 powered by Apache Tomcat Webmin or subsequent.

PRODUCT SPECIFIC INFORMATION
HP-UX Software Assistant:
HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Revision: 1 (rev.1) - 02 October 2007 Initial release

Third Party Security Patches:
Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01123426

Version: 2

HPSBUX02251 SSRT071449 rev.2 - HP-UX Running BIND, Remote DNS Cache Poisoning

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-01

Last Updated: 2007-09-10

Potential Security Impact: Remote DNS cache poisoning

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential vulnerability has been identified with HP-UX running BIND. The vulnerability could be exploited remotely to cause DNS cache poisoning.

References: CVE-2007-2926

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running BIND v9.2 or BIND v9.3

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

For BIND v9.2.0

HP-UX B.11.11
==========
BINDv920.INETSVCS-BIND
->action: install BIND920_v10.depot

HP-UX B.11.23
==========
InternetSrvcs.INETSVCS2-RUN
->action: install PHNE_36973 or subsequent

For BIND v9.3.2

HP-UX B.11.11
==========
BindUpgrade.BIND-UPGRADE
->action: install revision C.9.3.2.2.0 or subsequent
URL:
http://h20293.www2.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=BIND

HP-UX B.11.23
==========
BindUpgrade.BIND2-UPGRADE
->action: install revision C.9.3.2.2.0 or subsequent
URL:
http://h20293.www2.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=BIND

HP-UX B.11.31
==========
NameService.BIND-RUN
action: install named binary file

END AFFECTED VERSIONS

RESOLUTION
HP has provided the following software updates and patches to resolve the vulnerability.

The patch is available from http://itrc.hp.com

The updates are available from
http://h20293.www2.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=BIND

->BIND v9.2.0 HP-UX B.11.11 contact HP Support to receive BIND920_v10.depot or upgrade to BIND v9.3.2 revision C.9.3.2.2.0 or subsequent

->BIND v9.2.0 HP-UX B.11.23 install PHNE_36973 or subsequent

->BIND v9.3.2 HP-UX B.11.11 install revision C.9.3.2.2.0 or subsequent

->BIND v9.3.2 HP-UX B.11.23 install revision C.9.3.2.2.0 or subsequent

BIND v9.3.2 HP-UX B.11.31 install named as discussed below

Until a patch or upgrade is released for HP-UX B.11.31, HP has made binary files available to resolve the vulnerability. Please use the following process to download and install the binary file.

1. Download the appropriate named file from this ftp site into a secure directory:
ftp://ss071449:ss071449@hprc.external.hp.com/

2. Unpack using gunzip and verify the cksum or md5sum:

1406468692 4225172 named_9.3.2_11.31IA
400611368 2269184 named_9.3.2_11.31PA

MD5 (named_9.3.2_11.31IA) = 9bd93b513fde895ebc32602824db3341
MD5 (named_9.3.2_11.31PA) = 81041c98b5699d90e0d90cca14f90d18

3. Stop the DNS server:

If named is normally started and stopped during system reboot, use this command:
/sbin/init.d/named stop

If rndc is in use, from the managing server issue this command:
rndc stop

If not using rndc enter this command as root on the system running named:
sig_named kill

4. Confirm that named is no longer running:

ps -ef | grep named
Ignore any lines containing 'grep named'.

5. Replace named with the appropriate downloaded file.

Confirm that the downloaded file has permissions/ower/group of '544 bin bin'. Set the ownership and permissions if necessary.

cp <downloaded file> /usr/sbin/named

6. Restart named

If named is normally started during the system reboot:
/sbin/init.d/named start

Otherwise, restart named using procedures established for the system.

MANUAL ACTIONS: Yes - NonUpdate

BIND v9.2.0 HP-UX B.11.11 - contact HP Support or upgrade to BIND v9.3.2

BIND v9.3.2 HP-UX B.11.31 - install named file

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY
Version: 1 (rev.1) - 1 August 2007 Initial release
Version: 2 (rev.2) - 10 September 2007 patch and updates available

Third Party Security Patches:
Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletins – Tru64

**COMMUNICATION - SECURITY BULLETIN Document ID: c00576921**

Version: 2

HPSBTU02083 SSRT051069 rev.2 - HP Tru64 Unix Secure Web Server (SWS 6.4.1 and earlier) PHP/XMLRPC, Remote Unauthorized Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-12-06

Last Updated: 2007-08-08

Potential Security Impact: Remote unauthorized execution of arbitrary code

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in the Secure Web Server for Tru64 UNIX (powered by Apache) 6.4.1 and earlier when running PHP/XMLRPC. The vulnerability could be exploited by a remote unauthorized user to execute arbitrary code.

References: CAN-2005-1921

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported versions of HP Tru64 UNIX are affected when running the Secure Web Server 6.4.1 and earlier:

HP Tru64 UNIX Version 5.1B-3
HP Tru64 UNIX Version 5.1B-2/PK4
HP Tru64 UNIX Version 5.1A PK6

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

RESOLUTION
HP has released Secure Web Server (SWS) 6.4.1a for Tru64 UNIX, which addresses the potential vulnerability.

Note: The SWS 6.4.1a kit applies to HP Tru64 UNIX Versions 5.1B-3, 5.1B-2/PK4, and 5.1A PK6.

Kit Location: http://h30097.www3.hp.com/internet/download.htm

Kit File: sws_v6_4_1a.tar.gz

Kit MD5 Checksum: 3000048bb9e39b02e95628741f62e37b

UPDATE HISTORY

Version:1 (rev.1) - 06 December 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01154600

Version: 1

HPSBTU02256 SSRT071449 rev.1 - HP Tru64 UNIX or HP Tru64 Internet Express running BIND, Remote DNS Cache Poisoning

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-29

Last Updated: 2007-08-29

Potential Security Impact: Remote DNS cache poisoning

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been reported on the HP Tru64 Operating System or HP Tru64 Internet Express (IX) when running BIND. The vulnerability could be exploited remotely to poison the DNS cache.

References: CVE-2007-2926

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected:

HP Tru64 UNIX v 5.1B-4
HP Tru64 UNIX v 5.1B-3
HP Internet Express for Tru64 UNIX (IX) v 6.6 running BIND

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

RESOLUTION
Until the update is available in the mainstream product release, HP is releasing the following setld-based patch kits publicly for use by any customer.

The resolutions contained in patch kits are targeted for availability in the following mainstream product release:

HP Tru64 UNIX v 5.1B-5
HP Internet Express for Tru64 UNIX v 6.7

The kits distribute the following:

BIND-9.2.8-P1

HP Tru64 UNIX v 5.1B-4
Prerequisite: HP Tru64 UNIX v 5.1B-4 PK6 (BL27)
Name: T64KIT1001268-V51BB27-ES-20070806.tar
Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001268-V51BB27-ES-20070806

HP Tru64 UNIX v 5.1B-3
Prerequisite: HP Tru64 UNIX v 5.1B-3 PK5 (BL26)
Name: T64KIT1001273-V51BB26-ES-20070809.tar
Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001273-V51BB26-ES-20070809

HP Internet Express for Tru64 UNIX v 6.6
Note: Customers who use IX v 6.6 running BIND should install the HP Tru64 UNIX ERP kit appropriate for their supported operating system version

HISTORY - Version:1 (rev.1) - 29 August 2007 Initial release.

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletins – Storage Management

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01112990**

Version: 1

HPSBST02243 SSRT071446 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-036 to MS07-041

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-07-17

Last Updated: 2007-07-17

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-036, MS07-037, MS07-038, MS07-039, MS07-040, MS07-041.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Storage Management Appliance v2.1 Software running on:
Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

Patches released by Microsoft after MS06-051 are covered by monthly Security Bulletins

For the full archived list of Microsoft security updates applicable for Storage Management Appliance software v2.1, please refer to the following Security Bulletins available on the IT Resource Center (ITRC) Web site: http://www.itrc.hp.com/service/cki/secBullArchive.do

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security Bulletin HPSBST02146
For patches released by Microsoft in 2004, MS04-001 to MS04-045 refer to Security Bulletin HPSBST02147
For patches released by Microsoft in 2005, MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148
For patches released by Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140

The Microsoft patch index archive and further details about all Microsoft patches can be found on the following Web site:
http://www.microsoft.com/technet/security/bulletin/summary.mspx

NOTE: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 Update Rollup 1 for Service Pack 4 and Storage Management Appliance v2.1 advisory at the following website:
http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=12169&prodSeriesId=315667

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 for SP4, if they have not been installed already

RESOLUTION
HP strongly recommends the immediate installation of all security patches that apply to third party software which is integrated with SMA software products supplied by HP, and that patches are applied in accordance with an appropriate patch management policy.

NOTE: Patch installation instructions are shown at the end of this table.

MS Patch Analysis / Action

MS07-036
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-037
Vulnerability in Microsoft Office Publisher 2007 Could Allow Remote Code Execution (936548) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-038
Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-039
Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-040
Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-041
Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:
http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

HISTORY - Version: 1 (rev.1) - 17 July 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01143196**

Version: 1

HPSBST02255 SSRT071456 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-042 to MS07-050

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-20

Last Updated: 2007-08-20

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-042, MS07-043, MS07-044, MS07-045, MS07-046, MS07-047, MS07-048, MS07-049, MS07-050.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Storage Management Appliance v2.1 Software running on:
Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

Patches released by Microsoft after MS06-051 are covered by monthly Security Bulletins

For the full archived list of Microsoft security updates applicable for Storage Management Appliance software v2.1, please refer to the following Security Bulletins available on the IT Resource Center (ITRC) Web site: http://www.itrc.hp.com/service/cki/secBullArchive.do

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security Bulletin HPSBST02146
For patches released by Microsoft in 2004, MS04-001 to MS04-045 refer to Security Bulletin HPSBST02147
For patches released by Microsoft in 2005, MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148
For patches released by Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140

The Microsoft patch index archive and further details about all Microsoft patches can be found on the following Web site:
http://www.microsoft.com/technet/security/bulletin/summary.mspx

NOTE: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 Update Rollup 1 for Service

Pack 4 and Storage Management Appliance v2.1 advisory at the following website:
http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=12169&prodSeriesId=315667

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 for SP4, if they have not been installed already

RESOLUTION
HP strongly recommends the immediate installation of all security patches that apply to third party software which is integrated with SMA software products supplied by HP, and that patches are applied in accordance with an appropriate patch management policy.

NOTE: Patch installation instructions are shown at the end of this table.

MS Patch Analysis / Action

MS07-042
Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-043
Vulnerability in OLE Automation Could Allow Remote Code Execution (921503) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-044
Vulnerability in Microsoft Excel Could Allow Remote Code Execution
(940965) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-045
Cumulative Security Update for Internet Explorer (937143) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.
Impacts only: Internet Explorer 6 SP1 - Or - Internet Explorer 5.01 SP4 To determine your IE version check the IE help page.

MS07-046
Vulnerability in GDI Could Allow Remote Code Execution (938829) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-047
Vulnerabilities in Windows Media Player Could Allow Remote Code Execution (936782) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-048
Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution
(938123) SMA does not have this component.

Patch will not run successfully. Customers should not be concerned with this issue

MS07-049
Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-050 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA Copy the patch to a floppy diskette or to a CD Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

Note: The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:
http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

HISTORY - Version: 1 (rev.1) - 20 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01172326

Version: 1

HPSBST02260 SSRT071471 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-051 to MS07-054

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-09-17

Last Updated: 2007-09-17

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-051, MS07-052, MS07-053, MS07-054.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Storage Management Appliance v2.1 Software running on:
Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

Patches released by Microsoft after MS06-051 are covered by monthly Security Bulletins

For the full archived list of Microsoft security updates applicable for Storage Management Appliance software v2.1, please refer to the following Security Bulletins available on the IT Resource Center (ITRC) Web site: http://www.itrc.hp.com/service/cki/secBullArchive.do

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security Bulletin HPSBST02146
For patches released by Microsoft in 2004, MS04-001 to MS04-045 refer to Security Bulletin HPSBST02147
For patches released by Microsoft in 2005, MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148
For patches released by Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140
The Microsoft patch index archive and further details about all Microsoft patches can be found on the following Web site:
http://www.microsoft.com/technet/security/bulletin/summary.mspx

NOTE: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 Update Rollup 1 for Service Pack 4 and Storage Management Appliance v2.1 advisory at the following website:
http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=12169&prodSeriesId=315667

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 for SP4, if they have not been installed already

RESOLUTION
HP strongly recommends the immediate installation of all security patches that apply to third party software which is integrated with SMA software products supplied by HP, and that patches are applied in accordance with an appropriate patch management policy.

NOTE: Patch installation instructions are shown at the end of this table.

MS Patch Analysis / Action

MS07-051
Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and

install.

MS07-052
Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (941522) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-053
Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege (939778) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-054
Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

Installation Instructions: (if applicable)

Download patches to a system other than the SMA Copy the patch to a floppy diskette or to a CD Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

Note: The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:
http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

HISTORY - Version: 1 (rev.1) - 17 September 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletin – HP ServiceGuard

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01091941**

Version: 1

HPSBGN02234 SSRT071435 rev.1 - HP ServiceGuard for Linux, Local Unauthorized Access, Increase in Privilege

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-06-26

Last Updated: 2007-07-01

Potential Security Impact: Local unauthorized access, increase in privilege

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP Serviceguard for Linux. The vulnerability could be exploited to allow local unauthorized access or to increase privilege.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP Serviceguard for Linux:

RedHatAS2.1/ES2.1 releases SG A.11.14.04, A.11.14.05, A.11.14.06 Serviceguard Cluster Object Manager B.02.01.02, B.02.01.03

RedHat3.0AS RedHat3.0ES releases SG A.11.16.04, A.11.16.05, A.11.16.06, A.11.16.07, A.11.16.08, A.11.16.09, A.11.16.10 Serviceguard Cluster Object Manager B.03.01.02

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

This vulnerability does not affect the SUSE versions of HP Serviceguard and Cluster Object Manager.

RESOLUTION
HP has provided the following software patches to resolve this vulnerability.

The patches are available for download from: http://itrc.hp.com/

Retrieve applicable patches and install using applicable Linux tools.

RedHat Enterprise Linux, release Serviceguard A.11.16.11

RedHat3.0AS RedHat3.0ES IA32 SGLX_00150
RedHat3.0AS RedHat3.0ES IA64 SGLX_00151
RedHat3.0AS RedHat3.0ES x86_64 SGLX_00152

RedHat4AS RedHat4ES IA32 SGLX_00121
RedHat4AS RedHat4ES IA64 SGLX_00122
RedHat4AS RedHat4ES x86_64 SGLX_00123

RedHat Enterprise Linux, release Cluster Object Manager B.03.01.03

RedHat3.0AS RedHat3.0ES IA32 SGLX_00153
RedHat3.0AS RedHat3.0ES IA64 SGLX_00154
RedHat3.0AS RedHat3.0ES x86_64 SGLX_00155

RedHat4AS RedHat4ES IA32 SGLX_00130
RedHat4AS RedHat4ES IA64 SGLX_00131
RedHat4AS RedHat4ES x86_64 SGLX_00132

RedHat Enterprise Linux, release Serviceguard A.11.14.07

RedHatAS 2.1, RedHatES 2.1 IA32 SGLX_00148

RedHat Enterprise Linux, release Cluster Object Manager B.02.01.04

RedHatAS 2.1, RedHatES 2.1 IA32 SGLX_00149

PRODUCT SPECIFIC INFORMATION - None

HISTORY - Version: 1 (rev.1) - 2 July 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletin – HP OpenVMS

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01174368**

Version: 1

HPSBOV02261 SSRT071449 rev.1 - HP OpenVMS running BIND, Remote DNS Cache Poisoning

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-09-19

Last Updated: 2007-09-19

Potential Security Impact: Remote DNS cache poisoning

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been reported with HP OpenVMS when running BIND v 9.2.1 or BIND v 9.3.1. The vulnerability could be exploited remotely to cause DNS cache poisoning.

References: CVE-2007-2926

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected when running BIND v 9.2.1 or BIND v 9.3.1:

HP TCP/IP Services for OpenVMS Alpha v 5.4 HP TCP/IP Services for OpenVMS Alpha v 5.5 HP TCP/IP Services for OpenVMS Alpha v 5.6 HP TCP/IP Services for OpenVMS I64 v 5.5 HP TCP/IP Services for OpenVMS I64 v 5.6

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

RESOLUTION
Until the update is available in the mainstream product release, the patch will be made available to customers via their standard HP support channels through the HP Customer Support Center.

The resolutions contained in patch kits are targeted for availability in the following mainstream product

release:

TCPIP for OpenVMS V5.4 ECO7 which is planned for release in HP-Q1FY08 TCPIP for OpenVMS V5.5 ECO3 which is not yet scheduled for release TCPIP for OpenVMS V5.6 ECO3 which is not yet scheduled for release

HISTORY - Version 1 (rev.1) - 19 September 2007 Initial release.

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletin – Miscellaneous

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01077597**

Version: 1

HPSBPI02228 SSRT071404 rev.1 - HP Instant Support - Driver Check Running on Windows XP, Remote Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-06-13

Last Updated: 2007-07-02

Potential Security Impact: Remote unauthorized access

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with an ActiveX control in HP Instant Support - Driver Check running on Microsoft Windows. The vulnerability could be remotely exploited to allow unauthorized access to the system.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Instant Support - Driver Check earlier than v1.5.0.3 running on Microsoft Windows XP, XP Professional, XP Home Edition, XP Tablet PC Edition

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks John Heasman of NGSSoftware (http://www.ngssoftware.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks Carlo Di Dato (aka shinnai) for reporting this vulnerability to security-alert@hp.com.

RESOLUTION

HP has provided the following software update to resolve this vulnerability:

HP Instant Support - Driver Check v1.5.0.3 or later

To update HP Instant Support - Driver Check, visit http://www.hp.com/go/drivercheck

On the initial screen, click [Check Now].

If there is a version of the ActiveX control older than 1.5.0.3, the next screen will explain that the control needs to be updated.

Click [Continue] to update the ActiveX control.

Close the HP Instant Support - Driver Check application or continue to use it.

PRODUCT SPECIFIC INFORMATION - None

HISTORY: Version 1 (rev.1) - 2 July 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletins – System Management

**HPSBMA02274 SSRT071445** rev.1 - HP System Management Homepage (SMH) for HP-UX, Remote Cross Site Scripting (XSS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-10-03

Last Updated: 2007-10-03

Potential Security Impact: Remote cross site scripting (XSS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP System Management Homepage (SMH) for HP-UX. These vulnerabilities could by exploited remotely to allow cross site scripting (XSS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) running on HP-UX B.11.11, B.11.23, and B.11.31.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Thijs Bosschert (Fox-IT) for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. For affected systems, verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
==========
SysMgmtHomepage.SMH-RUN
action: install PHSS_36869 or subsequent

HP-UX B.11.23
==========
SysMgmtHomepage.SMH-RUN
action: install PHSS_36870 or subsequent

HP-UX B.11.31
==========
SysMgmtHomepage.SMH-RUN
action: install PHSS_36871 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has provided the following patches to resolve these vulnerabilities.
The patches are available from http://itrc.hp.com

HP-UX B.11.11 PHSS_36869 or subsequent
HP-UX B.11.23 PHSS_36870 or subsequent
HP-UX B.11.31 PHSS_36871 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY: Version:1 (rev.1) - 3 October 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01183597

Version: 1

HPSBMA02275 SSRT071445 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Cross Site Scripting (XSS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-10-03

Last Updated: 2007-10-03

Potential Security Impact: Remote cross site scripting (XSS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP System Management Homepage (SMH) for Linux and Windows. These vulnerabilities could by exploited remotely to allow cross site scripting (XSS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) versions prior to v2.1.10 running on Linux and Windows.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Thijs Bosschert (Fox-IT) for reporting this vulnerability to security-alert@hp.com.

RESOLUTION
HP has provided System Management Homepage (SMH) v2.1.10 or subsequent to resolve these vulnerabilities. The current version, SMH v2.1.10-186, is available from the following web sites:

HP System Management Homepage for Linux (x86) v2.1.10-186 can be downloaded from
http://h18007.www1.hp.com/support/files/server/us/download/27627.html

HP System Management Homepage for Linux (AMD64/EM64T) v2.1.10-186 can be downloaded from
http://h18007.www1.hp.com/support/files/server/us/download/27626.html

HP System Management Homepage for Windows v2.1.10-186 can be downloaded from
http://h18023.www1.hp.com/support/files/server/us/download/27540.html

Note: Two HP System Management Homepage for Windows v2.1.10.186 files are available, one localized for English and one localized for Japanese. One file is available for HP System Management Homepage for Linux (x86) and one file is available for HP System Management Homepage for Linux (AMD64/EM64T). Each Linux file contains the localizations for both English and Japanese.

HP System Management Homepage v2.1.10-186 is also available in the following ProLiant Support Packs.

ProLiant Support Pack for Red Hat Enterprise Linux 5 version 7.90
http://h18023.www1.hp.com/support/files/server/us/download/27567.html

ProLiant Support Pack for Microsoft Windows Server 2003 version 7.90 A
http://h18023.www1.hp.com/support/files/server/us/download/27534.html

PRODUCT SPECIFIC INFORMATION

HISTORY: Version:1 (rev.1) - 3 October 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01164065

Version: 1

HPSBMA02258 SSRT071470 rev.1 - HP System Management Homepage (SMH) for Windows, Incomplete Update Installation

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-09-10

Last Updated: 2007-09-12

Potential Security Impact: Incomplete update installation

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP System Management Homepage (SMH) for Windows on systems which are also running HP Version Control Agent (VCA) or Version Control Repository Manager (VCRM). The vulnerability may result in the incomplete installation of OpenSSL updates, including security updates.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) on Windows systems which are also running HP Version Control Agent (VCA) or Version Control Repository Manager (VCRM)

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

Updates to HP System Management Homepage (SMH) on Windows systems which are also running HP Version Control Agent (VCA) or Version Control Repository Manager (VCRM) may leave the previous OpenSSL software active in memory until the system is rebooted.

RESOLUTION
To avoid leaving potentially vulnerable OpenSSL software active in memory, always reboot a Windows system running SMH and VCA or VCRM immediately after installing an update to SMH.

HISTORY: Version:1 (rev.1) - 12 September 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01118771**

Version: 1

HPSBMA02250 SSRT061275 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Execution of Arbitrary Code and Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-01

Last Updated: 2007-08-01

Potential Security Impact: Remote execution of arbitrary code and Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified HP System Management Homepage (SMH) for Linux and Windows. These vulnerabilities could by exploited remotely resulting in the execution of arbitrary code or a Denial of Service (DoS).
References: CVE-2006-2937, CVE-2006-2940, CVE-2006-3738, CVE-2006-3747, CVE-2006-4339, CVE-2006-4343

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) versions prior to 2.1.7 running on Linux and Windows.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

RESOLUTION
HP has provided System Management Homepage (SMH) version 2.1.7 or subsequent for each platform to resolve this issue. A more recent version is available: System Management Homepage (SMH) version 2.1.8

HP System Management Homepage for Linux (x86) version 2.1.8-177 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26864.html

HP System Management Homepage for Linux (AMD64/EM64T) version 2.1.8-177 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26866.html

HP System Management Homepage for Windows version 2.1.8-179 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26977.html

HISTORY: Version:1 (rev.1) - 1 August 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

# HP Security Bulletins – HP OpenView

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00727143**

Version: 5

HPSBMA02133 SSRT061201 rev.5 - HP Oracle for OpenView (OfO) Critical Patch Update

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-07-19

Last Updated: 2007-07-18

Potential Security Impact: Local or remote compromise of confidentiality, availability, integrity.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Oracle(r) has issued a Critical Patch Update which contains solutions for a number of potential security vulnerabilities. These vulnerabilities may be exploited locally or remotely to compromise the confidentiality, availability or integrity of Oracle for OpenView (OfO).

References: Oracle Critical Patch Update - July 2007

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Oracle for OpenView (OfO) v8.1.7 or v9.1.01 or v9.2 running on HP-UX, Tru64 UNIX, Linux, Solaris, and Windows.

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

Oracle is a registered U.S. trademark of the Oracle Corporation, Redwood City, California.

Oracle has issued Critical Patch Update - July 2007.

For more information:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2007.html

Information about previous Oracle Critical Patch Updates can be found here:
http://www.oracle.com/technology/deploy/security/alerts.htm

The following products are affected:

Product Number Description

ORA200BC OfO v8.1.7 for HP-UX LTU
ORA200CA OfO v9.2 64bit HP-UX 11&11.11 LTU
ORA205BC OfO v8.1.7 for HP-UX 5 LTU Bundle
ORA205CA OfO v9.2 64bit HP-UX 11&11.11 5 LTUs
ORA230BC OfO v8.1.7 for HP-UX Media

ORA230CA OfO v9.2 64bit HP-UX 11&11.11 Media Kit
ORA240BC OfO v8.1.7 for HP-UX Eval LTU & Media
ORA300BC OfO v8.1.7 for Win 2000/NT LTU
ORA300CA OfO v9.2 32bit Windows LTU
ORA305BC OfO v8.1.7 for Win 2000/NT 5 LTU Bundle
ORA305CA OfO v9.2 32bit Windows 5 LTUs
ORA330BC OfO v8.1.7 for Win 2000/NT Media
ORA330CA OfO v9.2 32bit Windows Media Kit
ORA340BC OfO v8.1.7 for Win 2000/NT Eval LTU
ORA400BC OfO v8.1.7 for Sun Solaris LTU
ORA400CA OfO v9.2 32bit Sun Solaris 2.7&2.8 LTU
ORA401CA OfO v9.2 64bit Sun Solaris 2.7&2.8 LTU
ORA405BC OfO v8.1.7 for Sun Solaris 5 LTU Bundle
ORA405CA OfO v9.2 32bit Sun Solaris 2.7&2.8 5 LTU
ORA406CA OfO v9.2 64bit Sun Solaris 2.7&2.8 5 LTU
ORA430BC OfO v8.1.7 for Sun Solaris Media
ORA430CA OfO v9.2 32bit Sun Solaris 2.7&2.8 Media
ORA431CA OfO v9.2 64bit Sun Solaris 2.7&2.8 Media
ORA440BC OfO v8.1.7 for Sun Solaris Eval LTU
ORA500CA OfO v9.1.01 64bit Tru64 V5.1a LTU Ent.Ed
ORA505CA OfO v9.1.01 64bit Tru64 V5.1a LTU
ORA530CA OfO v9.1.01 64bit Tru64 V5.1a Media Kit
ORA600CA OfO for Linux LTU
ORA605CA OfO for Linux LTU Service Bureaus Bundle
ORA630CA OfO v9.2.0 for Linux, Media Kit

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23

action: If Oracle for OpenView (OfO) is installed, install the Oracle Critical Patch Update - July 2007

END AFFECTED VERSIONS

Note: Since Oracle for OpenView (OfO) is not installed using swinstall(1M) the Security Patch Check Tool cannot determine whether it is present on an HP-UX system. Customer maintained configuration documentation should be consulted to determine whether Oracle for OpenView (OfO) is installed.

RESOLUTION

Oracle for OpenView (OfO) customers who have support contracts directly with Oracle should obtain the "Critical Patch Update - July 2007" from Oracle.

Oracle for OpenView (OfO) customers who have support with Hewlett-Packard should contact their normal support channel to obtain the "Critical Patch Update - July 2007."

For support contract information, please visit:
http://www.hp.com/managementsoftware/contract_maint

MANUAL ACTIONS:

Yes – Update - Install the Oracle Critical Patch Update - July 2007.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY

Version:1 (rev.1) - 19 July 2006 Initial release "Critical Patch Update - July 2006"
Version:2 (rev.2) - 23 October 2006 "Critical Patch Update - October 2006" is available
Version:3 (rev.3) - 22 January 2007 "Critical Patch Update - January 2007" is available
Version:4 (rev.4) - 18 April 2007 "Critical Patch Update - April 2007" is available
Version:5 (rev.5) - 18 July 2007 "Critical Patch Update - July 2007" is available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01106515

Version: 1

HPSBMA02235 SSRT061260 rev.1 - HP OpenView Internet Service (OVIS) Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Internet Service (OVIS) running Shared Trace Service on HP-UX, Linux, Solaris, and Windows. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Internet Service (OVIS) v6.00, v6.10, v6.11 (Japanese), v6.20 running HP OpenView Cross Platform Component (XPL) vB.60.81.00, vB.60.90.00, and vB.61.90.000 on HP-UX, Linux, Solaris, and Windows

BACKGROUND
For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs

(dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL: http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the applicable hotfixes from the following url: as above

MANUAL ACTIONS: Yes - NonUpdate - Install the hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01109171

Version: 1

HPSBMA02236 SSRT061260 rev.1 - HP OpenView Performance Manager (OVPM) Running Shared Trace Service on HP-UX, Solaris, and Windows, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Performance Manager (OVPM) running Shared Trace Service on HP-UX, Solaris, and Windows. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Performance Manager (OVPM) 5.x and 6.x running on HP-UX PA-RISC and IPF (B.11.11,B.11.23), Solaris (5.7, 5.8, 5.9), Windows (2000, 2003 and Windows XP).

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.23 (IA)
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL: http://openview.hp.com/ecare/getsupportdoc?docid=QXCR1000390205

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL: as above

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the hotfix for QXCR1000390205: as above

MANUAL ACTIONS: Yes – NonUpdate Install the hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01109584

Version: 1

HPSBMA02237 SSRT061260 rev.1 - HP OpenView Performance Agent (OVPA) Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Performance Agent (OVPA) running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Performance Agent (OVPA) 4.5 and 4.6 running on AIX (5L,5.1,5.2(Power3,4),5.3), HP Tru64 UNIX (5.1A,5.1B), HP-UX (B.11.11,B.11.23),
Linux: Debian Linux (3.0 and later), Redhat Linux (AS/ES/WS 2.1 and later), SuSE (9.0 and later), Turbo Linux (8.x and later), Solaris (5.7, 5.8, 5.9,10), Windows (2000,2003 and XP).

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.23 (IA)
HPOvLcore.HPOVXPL
action: install revision 3.10.012 or subsequent
URL: http://openview.hp.com/ecare/getsupportdoc?docid=QXCR1000390205

HP-UX B.11.23 (PA)
HP-UX B.11.11
HPOvLcore.HPOVXPL
action: install revision 3.10.012 or subsequent
URL:  as above

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the hotfix for QXCR1000390205:  as above

MANUAL ACTIONS: Yes – NonUpdate - Install the hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see:  https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01109617

Version: 1

HPSBMA02238 SSRT061260 rev.1 - HP OpenView Reporter Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Reporter running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Reporter 3.7 running on Windows (2000, 2003, XP).

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the hotfix for QXCR1000390205:
http://openview.hp.com/ecare/getsupportdoc?docid=QXCR1000390205

PRODUCT SPECIFIC INFORMATION

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01110576

Version: 2

HPSBMA02239 SSRT061260 rev.2 - HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-28

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in HP OpenView Operations (OVO) Agents running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: -> CVE-2007-3872

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView OVO Agents OVO8.x HTTPS agents on AIX, HP-UX (IA and PA), HP Tru64 Unix, Solaris, and Windows running Shared Trace Service.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

-> Note: HP OpenView Operations (OVO) requires HP OpenView Network Node Manager (OV NNM) on the OVO server. OVO will install OV NNM if it is not already present. OV NNM requires the installation of certain patches to be compatible with the resolution discussed below. To insure correct operation the recommendations of Security Bulletin HPSBMA02242 SSRT061260 must be implemented before the recommendations of this Security Bulletin.

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
OVO-CLT.OVO-UX11-CLT
action: install revision 3.10.040 or subsequent
URL: http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

OVO-CLT.OVO-UXIA-CLT
action: install revision 3.10.040 or subsequent
URL: as above

OVO-CLT.OVO-SOL-CLT
action: install revision 3.10.040 or subsequent
URL: as above

OVO-CLT.OVO-WIN-CLT
action: install revision 3.10.040 or subsequent
URL: as above

OVO-CLT.OVO-LIN-CLT
->action: install PHSS_36278 or subsequent

OVO-CLT.OVO-AIX-CLT
action: install revision 3.10.040 or subsequent
URL: as above

OVO-CLT.OVO-TRU-CLT
->action: install PHSS_35457 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve the vulnerability. The patches can be downloaded from http://itrc.hp.com

Patches are not yet available for all client systems. For client systems without resolution patches available, HP has provided a hotfix to resolve this vulnerability.

Please contact HP Support and request the applicable hotfixes from the following url:

http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

Each patch is to be installed on the operating system listed in the "System to be Patched" column. Each patch is for communication with the operating system listed in the "Client System" column.

Patch (or subsequent) System to be Patched Client System
Install hotfix HP-UX PA HP-UX PA
Install hotfix HP-UX PA HP-UX IA
Install hotfix HP-UX PA Solaris
Install hotfix HP-UX PA Windows
PHSS_36278 HP-UX PA Linux
Install hotfix HP-UX PA AIX
->PHSS_35457 HP-UX PA Tru64 Unix
Install hotfix Solaris HP-UX PA
Install hotfix Solaris HP-UX IA
Install hotfix Solaris Solaris
Install hotfix Solaris Windows
ITOSOL_00586 Solaris Linux
Install hotfix Solaris AIX
->ITOSOL_00530 Solaris Tru64 Unix

MANUAL ACTIONS: Yes – NonUpdate - Install hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY
Version:1 (rev.1) - 7 August 2007 Initial release
Version:2 (rev.2) - 28 August 2007 Added OV NNM information, added CVE-2007-3872 to the references, PHSS_35457, ITOSOL_00530 available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01111851

Version: 1

HPSBMA02241 SSRT061260 rev.1 - HP OpenView Service Quality Manager (OV SQM) Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Service Quality Manager (OV SQM) running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Quality Manager (OV SQM) v1.2 SP1, v1.3, v1.40 running HP OpenView Cross Platform Component (XPL) 2.60.041, 2.61.060 and 2.61.110 on HP-UX and Windows

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL: http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the applicable hotfixes from the following url: as above

MANUAL ACTIONS: Yes – NonUpdate - Install the hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch

management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01112038

Version: 2

HPSBMA02242 SSRT061260 rev.2 - HP OpenView Network Node Manager (OV NNM) Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-16

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM) running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
-> HP OpenView Network Node Manager (OV NNM) v6.41, v7.01, v7.50, v7.51
running XPL earlier than 03.10.040 on HP-UX, Solaris, Windows NT, Windows 2000, Windows XP, and Linux

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if HP-UX has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.00
HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
HPOvLcore.HPOVXPL
action: install the XPL_COMPONENT_3.10.040 as discussed in the Resolution section

END AFFECTED VERSIONS

RESOLUTION
HP has made the following procedure available to resolve the vulnerability.

1. Install the following patches. These patches are available on: http://itrc.hp.com

OV NNM v6.41
HP-UX (PA) PHSS_35830 or subsequent
Solaris PSOV_03469 or subsequent
Windows 2000, Windows XP NNM_01148 or subsequent

OV NNM v7.01
HP-UX (PA) PHSS_35579 or subsequent
Solaris PSOV_03468 or subsequent
Windows 2000, Windows XP NNM_01147 or subsequent

-> OV NNM v7.50
HP-UX (PA) Upgrade to NNM v7.51 and install PHSS_36385 or subsequent HP-UX (IA) Upgrade to NNM v7.51 and install PHSS_36386 or subsequent Solaris Upgrade to NNM v7.51 and install PSOV_03479 or subsequent Windows 2000, Windows XP Upgrade to NNM v7.51 and install NNM_01158 or subsequent Linux RedHatAS2.1 Upgrade to NNM v7.51 and install LXOV_00052 or subsequent

-> OV NNM v7.51
HP-UX (PA) PHSS_36385 or subsequent
HP-UX (IA) PHSS_36386 or subsequent
Solaris PSOV_03479 or subsequent
Windows 2000, Windows XP NNM_01158 or subsequent Linux RedHatAS2.1 LXOV_00052 or subsequent

Note: The patches listed above do not resolve the vulnerability. They are needed for compatibility with XPL 03.10.040, which does resolve the vulnerability.

2. Download the appropriate XPL_COMPONENT_3.10.040 file from the following site into a secure directory:
ftp://cme_xpl:0310040@hprc.external.hp.com/

HP-UX (PA-RISC) XPL_COMPONENT_3.10.040_HPUX.tar.gz
HP-UX (Itanium) XPL_COMPONENT_3.10.040_IPF.tar.gz Linux (RHEL2.1 AS) XPL_COMPONENT_3.10.040_Linux.tar.gz
Solaris PL_COMPONENT_3.10.040_SOL.tar.gz Windows XPL_COMPONENT_3.10.040_Win.zip

3. Unpack the gz files using gunzip.

4. Verify the cksum or md5sum:
765964855 13967360 XPL_COMPONENT_3.10.040_HPUX.tar
964115406 22978560 XPL_COMPONENT_3.10.040_IPF.tar
1071892883 2324480 XPL_COMPONENT_3.10.040_Linux.tar
2657852015 11857920 XPL_COMPONENT_3.10.040_SOL.tar
1507786934 1510091 XPL_COMPONENT_3.10.040_Win.zip
MD5 (XPL_COMPONENT_3.10.040_HPUX.tar) = 15cfc5f312ea192fcef5acf1f71b0f8a
MD5 (XPL_COMPONENT_3.10.040_IPF.tar) = 86743b9a9585915f20e31c7da85fda69
MD5 (XPL_COMPONENT_3.10.040_Linux.tar) = 1c30fae89c3682e5bb7d7e2747fcd734
MD5 (XPL_COMPONENT_3.10.040_SOL.tar) = 4cd395f2f5b4a3c8aef34131643c1751
MD5 (XPL_COMPONENT_3.10.040_Win.zip) = 3504a9c04b7f8f9502455043e07fb29d

5. Unpack the tar or zip file into a secure directory.

6. Execute the appropriate installation script: install.sh or install.bat.

MANUAL ACTIONS: Yes - Install XPL_COMPONENT_3.10.040.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY
Version: 1 (rev.1) - 7 August 2007 Initial release
Version: 2 (rev.2) - 16 August 2007 Added NNM v7.51

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01114023

Version: 1

HPSBMA02244 SSRT061260 rev.1 - HP OpenView Business Process Insight and Related Products Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with the HP OpenView Business Process Insight family of products running Shared Trace Service on Windows. The vulnerability could be remotely exploited to execute arbitrary code. The HP OpenView Business Process Insight family of products includes HP OpenView Business Process Insight (OVBPI),HP Business Process Insight (HPBPI) , HP OpenView Service Desk Process Insight (SDPI), and HP Service Desk Process Insight (HPSDPI).

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Business Process Insight (OVBPI), HP Business Process Insight (HPBPI) , HP OpenView Service Desk Process Insight (SDPI), and HP Service Desk Process Insight (HPSDPI) versions 1.0, 1.1x, 2.0x and 2.10x on Windows running Shared Trace Service from the HP OpenView Cross Platform Component prior to v3.10.040.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the "HP OpenView Cross Platform Component" in the Add/Remove program list. If the version listed in the Support Information is earlier than 3.10.040, install the patch as described in the Resolution section (below).

RESOLUTION
HP has provided the following patch to resolve this vulnerability.

OVBPI_00014 or subsequent

The patch is available from:
http://support.openview.hp.com/patches/ovbpi/02.10/win.jsp

Download the patch which contains an install image of the HP OpenView Cross Platform Component (XPL) containing the Shared Trace Service. Execute the installer and follow the onscreen instructions.

Note: By default the HP Business Process Insight family installer does not install the affected Shared Trace Service component. It is installed by explicitly running the XPL installer included on the HPBPI media. It may also have been installed it along with another HP OpenView software product. Please check with the support channel to see if other HP OpenView components on the system may be affected.

PRODUCT SPECIFIC INFORMATION

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

## SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01114156

Version: 1

HPSBMA02245 SSRT061260 rev.1 - HP OpenView Dashboard Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Dashboard running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Dashboard v2.01 running HP OpenView Cross Platform Component (XPL) vB.60.90.00 and vB.61.90.000 on Windows, Solaris and HP-UX.

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL:
http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the applicable hotfixes from the following url: as above

MANUAL ACTIONS: Yes – NonUpdate - Install the hotfix

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01115068**

Version: 1

HPSBMA02246 SSRT061260 rev.1 - HP OpenView Performance Insight (OVPI) Running Shared Trace Service, Remote Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-08-07

Last Updated: 2007-08-07

Potential Security Impact: Remote arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Performance Insight (OVPI) running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Performance Insight (OVPI) v5.0, v5.1, v5.1.1, v5.1.2, v5.2 running HP OpenView Cross Platform Component (XPL) earlier than v3.10.040 on HP-UX Precision Architecture (PA), HP-UX Itanium (IA), Linux, Solaris, and Windows

BACKGROUND
For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@hp.com.

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
HPOvLcore.HPOVXPL
action: install revision 3.10.040 or subsequent
URL: http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

END AFFECTED VERSIONS

RESOLUTION
HP has provided a hotfix to resolve this vulnerability. Please contact HP Support and request the applicable hotfixes from the following url: as above

MANUAL ACTIONS: Yes – NonUpdate - install revision 3.10.040 or subsequent

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY - Version: 1 (rev.1) - 7 August 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

## HP Security Bulletin – HP JetDirect

**SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00557788**
Version: 2

HPSBPI02078 SSRT5979 rev.2 - HP Jetdirect 635n IPv6/IPsec Print Server (J7961A), Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2005-11-15

Last Updated: 2007-08-08

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Potential vulnerabilities have been identified with the HP Jetdirect 635n IPv6/IPsec Print Server (J7961A) .

These vulnerabilities may be exploited remotely by an unauthorized user to create a Denial of Service (DoS).

References: NISCC Vulnerability Advisory 273756

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP Jetdirect 635n IPv6/IPsec Print Server (J7961A) running firmware versions prior to J7961A V.31.08

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

RESOLUTION

HP is providing a firmware update, J7961A V.31.08, to resolve this issue. The firmware can be updated using the HP Download Manager application.

The HP Download Manager application can be downloaded from http://www.hp.com/go/dlm_sw

UPDATE HISTORY

Version:1 (rev.1) - 15 November 2005 Initial release
Version:2 (rev.2) - 08 August 2007 Reformatted

# Secunia Advisory - HP-UX 11.11 ldcconn Buffer Overflow Vulnerability

**HP-UX 11.11 ldcconn Buffer Overflow Vulnerability**

SECUNIA ADVISORY ID: SA26373

09 August 2007 16:30

VERIFY ADVISORY: https://ca.secunia.com/?page=viewadvisory&vuln_id=26373

CRITICAL: Moderately critical

IMPACT: DoS, System access

WHERE: From local network

OPERATING SYSTEM: HP-UX 11.x

http://secunia.com/product/138/

DESCRIPTION: A vulnerability has been reported in HP-UX, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in ldcconn and can be exploited to cause a buffer overflow by sending an overly long string to the service (default port 17781/TCP).

Successful exploitation allows execution of arbitrary code.

The vulnerability is reported in the HP Controller for Cisco Local Director package on HP-UX 11.11i.

SOLUTION: The vendor recommends using another tool as the package has been obsolete since 2002 and is no longer supported.

PROVIDED AND/OR DISCOVERED BY: iDefense Labs

ORIGINAL ADVISORY:

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=572

---

Secunia recommends that you verify all advisories you receive by following the link to:
https://ca.secunia.com/

Secunia NEVER sends attached files with advisories.

Secunia does not advise people to install third party patches, only use those supplied by the vendor.

Secunia is not responsible for the direct or indirect consequences of applying solutions or workarounds. All solutions and workarounds must be tested according to your internal company guidelines before being applied to production systems.

Secunia does not endorse or guarantee the integrity or intentions of any third party sites, following links to third party sites is solely your own responsibility.

Secunia can not be held liable for any issues related to the use or misuse of exploit code linked to from this advisory.

Secunia can not be held liable for any damages caused by visiting third party sites.

ABOUT SECUNIA AND SECUNIA ADVISORIES:

Definitions: (Criticality, Where etc.)

https://ca.secunia.com/?page=vdb_about_advisories

Manage your profile at Secunia: https://ca.secunia.com/

Contact details:

Web : http://corporate.secunia.com/
E-mail : cstsupport@secunia.com
Tel : +45 7020 5144
Fax : +45 7020 5145

## Australian CERT – OpenView for Windows

**HP OpenView for Windows - Hewlett-Packard OpenView Operations**
**From the Australian CERT**

http://www.auscert.org.au/render.html?it=7955

AL-2007.0093 - AUSCERT ALERT
Hewlett-Packard OpenView Operations OVTrace Buffer Overflow Vulnerabilities
10 August 2007

AusCERT Alert Summary

Product: Hewlett-Packard OpenView Operations

Publisher: iDefense
Operating System: Windows
Impact: Administrator Compromise
Access: Remote/Unauthenticated
CVE Names: CVE-2007-3872

Original Bulletin:

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=574

Hewlett-Packard OpenView Operations OVTrace Buffer Overflow Vulnerabilities

iDefense Security Advisory 08.09.07
http://labs.idefense.com/intelligence/vulnerabilities/
Aug 09, 2007

I. BACKGROUND

OpenView Operations software is a suite of network management tools used to monitor events on, and evaluate the performance of, hosts on the network. The OVTrace component of this suite is used to log the actions being taken by the other components of the suite in order to debug any problems that may be occurring. More information can be found at the following link.

http://h20229.www2.hp.com/products/ovowin/index.html

II. DESCRIPTION

Remote exploitation of multiple stack-based buffer overflow vulnerabilities in Hewlett-Packard Development Co.'s OpenView Operations for Windows OVTrace service may allow an attacker to execute arbitrary code with SYSTEM privileges.

The vulnerabilities exist within functions responsible for handling requests. These functions take a string from the request and copy it into fixed-size stack buffers. Since the length has not been properly validated, this results in an exploitable stack-based buffer overflow.

III. ANALYSIS

Exploitation of these vulnerabilities results in arbitrary code execution with SYSTEM privileges.

The OVTrace service, while not crucial to normal operations, is started by default. The OVTrace service is also present on systems that have only the management console installed as well as systems that have a full installation of the server and console installed.

IV. DETECTION

iDefense has confirmed the existence of these vulnerabilities in HP OpenView version A.07.50 for Windows, with all patches applied as of Jun 27, 2007. Previous versions may also be affected.

V. WORKAROUND

Employing firewalls to limit access to the affected service will mitigate exposure to these vulnerabilities.

VI. VENDOR RESPONSE

Hewlett-Packard Co. has addressed these vulnerabilities by releasing patches for all HP OpenView

products that contain the Shared Trace Service component. For more information consult the following HP Support Documents; c01106515, c01109171, c01109584, c01109617, c01110576, c01110627, c01111851, c01112038, c01114023, c01114156, c01115068 at the URLs shown below.

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01106515

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109171

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109584

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109617

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01110576

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01110627

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01111851

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01112038

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01114023

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01114156

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01115068

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2007-3872 to this issue. This is a candidate for inclusion in the CVE list (http://cve.mitre.org/), which standardizes names for security problems.

VIII. DISCLOSURE TIMELINE

07/12/2007 - Initial vendor notification
07/13/2007 - Initial vendor response
08/09/2007 - Coordinated public disclosure

IX. CREDIT

The discoverer of these vulnerabilities wishes to remain anonymous.

Get paid for vulnerability research:

http://labs.idefense.com/methodology/vulnerability/vcp.php

Free tools, research and upcoming events:

http://labs.idefense.com/

X. LEGAL NOTICES



With thanks to Mike Ellison