EPING December 2007

This is an archived edition of EPing, first published in December 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 -

Peace and Goodwill to All Data Centre Managers

Here's a little known fact – worldwide data centres account for as much carbon emission as the airline industry. Sooner, rather than later, people outside our industry will realise this and the spotlight will be even more tightly focussed on what 'we' do with 'all those computers'. Of course we only run those computers to provide a service to everyone else, but without doubt the IT industry will be called to account.

So spare a thought for your data centre manager in all this. They are caught in the cross-fire between the need to cut emissions (most probably seen within the company as the need to reduce energy costs which are rising rapidly) and our demands for more servers and more space and power. If and when we implement more services on blades the problems are likely to get worse. Blades may reduce space requirements but this is usually accompanied by an increase in the weight of racks – is your floor strong enough? And blades concentrate the power and the heat into a smaller area, possibly creating hot spots within your machine room that the air conditioners will struggle to cope with. They will increase their power consumption in an attempt to adapt and up goes your energy bill and carbon footprint again.

This is not to say that I am against the introduction of blades – far from it. But what it does highlight is that we are at a transition point with respect to the design for cooling in the data centre. Traditional designs with large air conditioning units on the sides of the room have been described as similar to cooling your whole kitchen just because you need a refrigerated area in one corner. Designs exist which bring the cooling much closer to the heat source, and as power densities in racks increase these may be worth considering. Making adaptations to your data centre could be a slow and laborious process, so don't get caught out!

And with that all that remains is for me to wish you all a Happy Christmas and a prosperous New Year and to thank everyone at hpUG, both staff and volunteers, for another year of sterling effort.

We hope you have enjoyed and benefited from your hpUG membership during the last year, and look forward to being in contact with you again during 2008.

And in case you haven't already guessed, the theme for this issue is Blades.

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

The Scripting Corner

by Bill Hassell

I have always used temporary files to store information that I will use several times in my script. This is especially true if the information takes a while to gather, for instance **ioscan** or **bdf**. After months of cleaning up these files, I developed an easy way to accomplish this by creating a temp directory and then using traps to remove the directory and anything inside the directory. The code template looks something like this:

```
umask 077
MYNAME=${0##*/}

# Check if common TEMP variables are set
# Set a default value if undefined

UNSET=IamNOTset
TEMP=${TEMP:-$UNSET}
TMPDIR=${TMPDIR:-$UNSET}
TEMPDIR=${TEMPDIR:-$UNSET}

# Now pick the temp directory:
#  Start with MYTEMPDIR=/var/tmp but change
#  MYTEMPDIR to a predefined temp directory
#  if one or more of the common Unix variables
#  have been set.

export MYTEMPDIR=/var/tmp/$MYNAME.$$
[ $TEMP = $UNSET ] || MYTEMPDIR=$TEMP/$MYNAME.$$
[ $TEMPDIR = $UNSET ] || MYTEMPDIR=$TEMPDIR/$MYNAME.$$
[ $TMPDIR = $UNSET ] || MYTEMPDIR=$TMPDIR/$MYNAME.$$

# In case there is an existing file or directory
# remove it first

[ -r $MYTEMPDIR ] && rm -rf $MYTEMPDIR
mkdir $MYTEMPDIR

trap 'rm -rf $MYTEMPDIR;exit' 0 1 2 3 11 15
```

The above code will create a temp directory and store the name in **$MYTEMPDIR**. So to create a temp file, you simply give the file any name you wish with a directory path **$MYTEMPDIR**. There are about 3 common environment variables that may (or may not) be preset depending on the system: **$TEMP** **$TMPDIR** and **$TEMPDIR**. If any of these are set, we should use that as the starting point for your temp directory (which this code will do).

The **umask** value is set for 700 directory permission, keeping the contents private to this user. And **MYNAME** is assigned the script's name using the shell equivalent of the **basename** command (**MYNAME=${0##*/}**).

The **$UNSET** variable and the subsequent assignments are used to test for a set variable without causing an error when set -u is in effect. **set -u** will abort the script when the contents of an undefined variable is read. Now **set -u** is a great tool to improve script reliability but the script still needs to determine if one of these variables is set. The conditional assignment statement (as in: **TEMP=${TEMP:-$UNSET}**) means that if the **TEMP** variable has not been defined, give a new value,

in this case **$UNSET**. Later on, we'll test the variable to see it was not set in the current environment. The variable **UNSET** is just a flag to use for this purpose.

Once we have established the path for the temp directory, the name of the directory will be the name of the script plus the process ID number (**PID**) which is stored in **$$**. Then just in case a leftover directory already exists, remove it and all the contents, then create the temp directory. Now just create files as needed with the path **$MYTEMPDIR**, for example:

```
bdf > $MYTEMPDIR/bdf.out
```

Well, that was a lot of details. And with the above template for all scripts, it is easy to use. However, for small files (a few megs), a much faster (and simpler) method is to simply assign the information to a variable, like this:

```
MYBDF=$(bdf)
```

No temp directory, no cleanup traps, and no filesystem overhead. The variable **MYBDF** will now have all the lines in memory and can be searched much faster than a file. The only caution is to remember to use **"$MYBDF"** to retain all the newline characters. The following will illustrate the difference:

```
MYBDF=$(bdf)

echo $MYBDF
Filesystem kbytes used avail %used Mounted on /dev/vg00/lvol3 143360 118840
24352 83% / /dev/vg00/lvol1 295024 78656 186864 30% /stand /dev/vg00/lvol8
2048000 185960 1855160 9% /var …

echo "$MYBDF"
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360  118840   24352   83% /
/dev/vg00/lvol1     295024   78656  186864   30% /stand
/dev/vg00/lvol8    2048000  185960 1855160    9% /var …
```

The first echo shows everything on one line while the second will look exactly like the original command and can be parsed the same way as with a temp file. Note: very large blocks of information will not be appropriate (more than a few megs) due to the maximum length of a variable (see **getconf ARG_MAX**). However, a very long bdf listing (for example) is less than 100KB.

BladeSystem Support Offerings

Hot off the Press – a Brochure on blade services which has been recently produced, summarising the HP BladeSystem support offerings.

For the brochure and part number matrix go to:

http://h41111.www4.hp.com/hps/carepack/uk/en/descriptions.html

With thanks to Hugh Williams

HP BladeSystems, VMware and Insight Control Care Pack Services, Hewlett Packard Ltd

OpenVMS expands support of HP BladeSystems

With the delivery of OpenVMS 8.3-1H1 Integrity in November 2007, OpenVMS has extended its support of the c-Class BladeSystems. New management software based on HP SIM (Systems Insight Manager), common to all HP platforms and WBEM (the open standard Web-Based Enterprise Management protocol) enables management and provisioning of OpenVMS Blades alongside HP-UX, Linux and Windows from a single 'pane of glass'. OpenVMS supports the c7000 BladeSystem housing up to 32 Cores (8 BL860c Blades) and by year-end the c3000 'Shorty' enclosure with up to 16 Cores (4 BL860c Blades).

For more about OpenVMS on Blades:

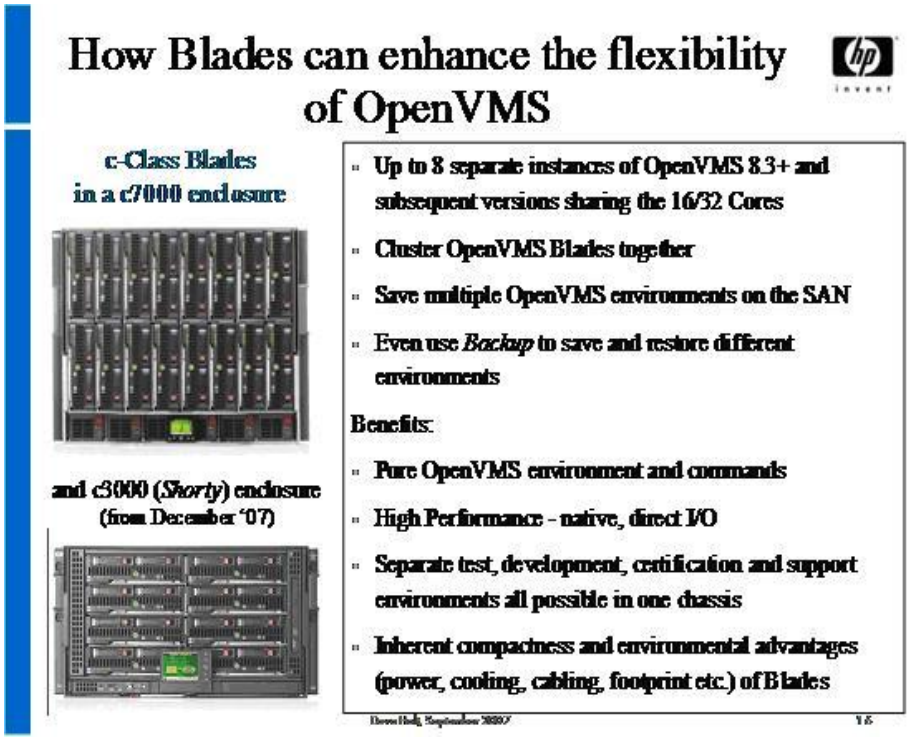
http://h18004.www1.hp.com/products/servers/Integrity-bl/c-class/860c/index.html

OpenVMS Blades Provisioning

Provisioning is the installing or upgrading of an operating system. With provisioning support, HP Systems Insight Manager (HP SIM) installs or upgrades the OpenVMS operating system quickly and easily on up to eight servers across the network simultaneously. Provisioning support also facilitates installing or upgrading OpenVMS on HP Integrity Blades and servers that do not include a CD/DVD drive.

For more information on OpenVMS Provisioning:

http://h71000.www7.hp.com/openvms/products/provisioning/index.html



HP BladeSystems

The c7000 and c3000 Blades enclosures have been designed from the ground up to deliver the future of scalable infrastructure design today and represent a significant leap forward. These products offer flexibility and scalability by allowing customers to manage server, storage, networking and power management as a unified environment. The BL860c features support for all four Integrity operating

environments, HP-UX 11i, OpenVMS, Windows and Linux – both Red Hat and SUSE – and Windows 32/64. By supporting Proliant server blades in the same enclosure, customers have the dual benefits of Integrity and Proliant applications running in the common chassis with common management.

Up to 8 separate instances of OpenVMS can be deployed in one BladeSystem c-Class enclosure, enabling different versions of OpenVMS and different tasks - development, support, testing, certification, production etc. - to be isolated from each other as required. OpenVMS BladeSystems can be clustered with other OpenVMS Blades and/or OpenVMS Integrity and AlphaServers with traditional OpenVMS clustering capabilities and performance.

The BL860c Server Blade is a key member of the BladeSystem c-Class family

The BL860c is a 2-socket, full-height, c-Class server blade featuring single- and dual-core Itanium® 2 Montecito or Madison processors. It supports up to 48GB of memory in 12 DIMM slots and utilizes the HP zx2 chipset. The BL860c features up to 2 internal SAS (Serial Attached SCSI) small-form-factor hard disk drives, 4 embedded 1:10Gb Gbit LAN ports as well as 3 mezzanine cards for a wide range of I/O support including Fibrechannel and InfiniBand fabrics. The hard disk drives and mezzanine cards are the same HDDs and I/O cards utilized by BladeSystem c-Class ProLiant server blades. BL860c server blades can be configured alongside other ProLiant server blades and HP storage blades in a single enclosure. The c3000 also includes a DVD drive.

Dave Holt
Hewlett-Packard Limited

HP Education Services for HP BladeSystems and Insight Control Environment training

HP has launched Insight Control Environment (ICE) as the most efficient and effective way to install, manage and maintain both ProLiant and Blade servers. In line with this new approach, HP Education Services has developed a new ICE curriculum covering all levels of training:

Introductory courses: WBT courses and a 2-day hands-on ICE Foundation class will help students understand the key elements of Insight Control Environment to manage, monitor, deploy and update HP BladeSystems and ProLiant servers, such as software install, licensing, software configuration, discovery and deployment.

HP BladeSystem administration: Training will teach students how to successfully deploy and manage HP BladeSystem server blades. The course encompasses connection of the HP BladeSystem servers to both network and external storage devices, along with specific training on Onboard Administrator and HP Virtual Connect.

Insight Control Environment management and monitoring: Training will provide students with in-depth knowledge of HP SIM, ILO and the associated architecture to perform essential administration tasks such as: installation, configuration and discovery, monitoring managed devices, managing storage, and using task, lists, tools, events and trusts.

Insight Control Environment deployment and update: Training will provide students with in-depth knowledge of HP RDP and its architecture to successfully deploy and maintain ProLiant servers. Students will use RDP, (the combination of Altiris' Deployment Solution and HP ProLiant Integration Module) to perform essential administration tasks such as software updates and license management.

For full curriculum and datasheets of all courses see:

http://h10076.www1.hp.com/education/curr-proliant-curriculum.htm

For the UK schedule for 2008 see:

http://h41156.www4.hp.com/education/courses.aspx?cc=uk&ll=en&group=231

Tony Shortland
HP Education Services

OpenVMS celebrates 30 years of tremendous success

See:

http://h71000.www7.hp.com/openvms/30th/index.html

Computerworld on OpenVMS 30th anniversary:

See:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9044560

NHS Supply Chain delivers with CONNX - A Case Study

This case study explains how NHS Supply Chain linked a Windows based voice activated warehouse picking system to their HP OpenVMS back end systems in a totally seamless yet real time manner.

For the full case study see:

http://h71000.www7.hp.com/success-stories.html

Below is a direct link to the pdf on one of HP's servers:

http://h71028.www7.hp.com/ERC/downloads/NHS_Supply_Chain_Generix_CONNX.pdf

Further information on CONNX can be found at:

http://www.connx-net.com

IT Pros Share their horror stories

HP Users Group Members tell of blue screens of death and what can happen when a UPS beeps
http://www.networkworld.com/news/2007/103007-it-pros-horror.html?page=1

hpUG Surveys and Congratulations to the Recent Winner

Did you miss out on a chance to win two prizes?

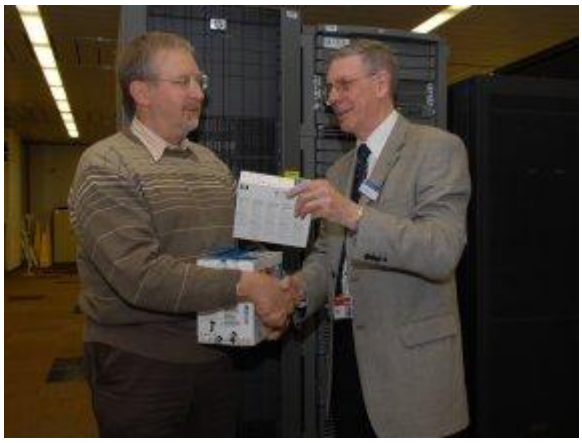
Prizes on offer for this autumn's survey were a Digital Camera (M527) AND a Photosmart Printer (A526)

This survey has now been completed, but we still want to know what you feel is good, bad or indifferent about hpUG – watch out for the next survey or email us.

Please mail all comments (good or bad) to admin@hpug.org.uk

CONGRATULATIONS to the winner of the two prizes - Richard Fisker

Richard started work with ECMWF in 1979 and is the Servers & Desktops Section Head. He has been using HP-UX servers since 1996. Currently he has two Highly Available clusters using Service Guard. The clusters are composed of 6 HP Integrity rx4640s, together with 3 EVA arrays. These systems are used for (a) HOME fileservers for all desktops and general purpose servers and (b) acquisition of weather observation and the dissemination of weather forecasts to our member states.



More details concerning ECMWF can be found at: www.ecmwf.int

Praise for hpUG Seminars

hpUG Seminar - "Data and Storage Networking" - 4 October 2007

To Gerald Hackemer, hpUG

I thought I should take this opportunity to drop you a note regarding the above seminar.

This is precisely the type of meeting I had hoped that the User Group would be putting on nowadays.

Several things stood out for me in the meeting of 4 October:

1/ the professionalism of Colin [Butcher]'s presentation: both knowledge of the subject area and his presentation skills
2/ the level of expectation from the attendees
3/ what appeared to me to be the total enthrallment of those present (nobody dropped off to sleep after lunch)
4/ the total lack of ANY marketing.

It is also obviously necessary that we have technical updates for new hardware and software features. We also need to have meetings to have new technologies explained. It is disappointing, however, to see how limited most people's view of the industry is and this is where the User Group can help.

It is my view that the technologies will be learnt or taught, by the companies who have staff to deploy them, but the general education through the User Group is much needed. Finding presenters who know the field and are skilled at presenting must be a difficult job, but worth the effort. This isn't what is taught in the usual tech ed training courses. We have too many people who are specialists, but don't have the "big picture".

I know that I have a somewhat peculiar view as I stand outside the mainstream now, but I hope that we can see more of these User Group events.

When you target a non-specific group but genuinely add to the attendees understanding of the underlying technologies this must be a winning formula.

Thanks again for putting together such a useful event.

Tim Pass, Control-X Ltd

Take a look at our events page for the latest information on hpUG forthcoming events:

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

hpUG Seminar Review

HP server and storage strategy update – 15 November 2007 - Warrington

The venue for this seminar was the HP Offices in Kelvin Close, Warrington. The day was run in partnership with Nike Consultants and Dai Davies started proceedings with an introduction to Nike's services and their history.

Next, from HP, Malcolm Cochran gave us the latest updates on the Integrity server and the Intel chips within, including some Intel details of the next generations of the CPU, features of the CPU and new supporting chipsets.

Euan McMaster from HP went on to describe the server offerings in more detail, power management and efficiency, and how the operating systems of OpenVMS, linux, Windows and HP-UX are evolving as a result, and a look at server management software. He looked closely at blade systems and how they are evolving and how they can be managed and used, describing how virtualization technology simplifies their deployment.

After an excellent lunch, Brynn Harrison of HP described the current and future storage offering in the XP, the EVA and the MSA storage arrays, comparing and contrasting their uses and operation, tape futures, and as usual overran due to the technical questions he always answers so well!

To round off, Euan talked about migration options for HP-UX to the Integrity which covered migrations services from HP and also non HP platforms.

All in all a fascinating day with Non Disclosure Agreement (NDA) material regrettably I cannot share. The event was thoroughly enjoyed and appreciated by those who attended.

Nic Clews for hpUG, Chair of the meeting

hpUG Seminars – Examples of Recent Offerings

hpUG Seminar - Data and Storage Networking - 4 October 2007

Seminar Description contained in the publicity prior to the event:

Data and storage networking are very similar. It is important to understand the underlying principles thoroughly, especially when designing and implementing critical infrastructure projects.

This seminar will discuss the various components involved in implementing networks and explain why they work as they do, thus helping to develop an understanding of their capabilities and limitations. The seminar will cover physical infrastructure (eg: cabling, fibre-optics), segmentation methods (eg: switching, VLANs, routing), network protocols (eg: TCP/IP, DECnet) and performance aspects (eg: latency, bandwidth, multiple paths).

The seminar will concentrate on ethernet and fibrechannel technologies, but will also cover other topics such as high performance inter-site links and wireless networks.

The seminar will use a typical mixed system split site infrastructure design 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.

Venue: The HP Offices, 88 Wood St., LONDON EC2V 7QT

Presenter: Colin Butcher is a well known systems consultant. He regularly presents educational seminars and intermittently writes articles for publication.

He has considerable experience of working with mission-critical systems and networks around the world and has strong links with HP OpenVMS Engineering.

hpUG seminar - HP Server & Storage Strategy Update - 15 November 2007

Seminar Description contained in the publicity prior to the event:

The pace of technological evolution is threatening to make long-term strategic planning one of the most important corporate development roles. Therefore HP is detailing their medium and long-term development plans so that you can develop your adaptive enterprise strategy from the most informed position..

This seminar will cover the development plans for each of the HP Server product lines, including Itanium, Blades and Industry Standard Servers, and the corresponding Operating Systems. It will

cover issues of server consolidation, from bringing legacy hp e3000, hp9000 and ISS to a single point of consolidation to the implementation of cross-platform data storage solutions. HP will also outline their exciting new Blade range, 4Gb EVA Switches and HBAs and provide an insight into how often exponentially growing datasets can be shared by the enterprise

Venue: Hewlett-Packard Ltd., 2 Kelvin Close, Birchwood Science Park, Risley, WARRINGTON, WA3 7PB

Presenters:

Euan McMaster is HP's UK Manager of the Alpha Retain Trust initiative and runs the UNIX Customer Care program in the U.K.

Malcolm Cochran is HP's Product Manager for AlphaServers, HP 9000, HP Integrity and the operating systems they support.

Brynn Harrison is an HP Technical Consultant specialising in: near-line systems, backup software, SAN infrastructure and online array systems

Dai Davies is the Business Development Manager for the BCS division of Nike Consultants.

hpUG Seminar - "Server Virtualisation" - 5 December 2007

Seminar Description contained in the publicity prior to the event:

The interest and developments around virtualisation in the x86 space have been high on the agenda over the past few years.

Although VMWare is the most dominant server virtualisation technology in the market place, there are emerging trends and technologies that can not be overlooked.

This seminar will cover the current trends and some emerging technologies. Including Xen and Citrix XenSource, Windows Server Virtualisation, HP's Virtual Server Environment and Virtual Connect.

Venue: The HP Offices, 88 Wood St., LONDON EC2V 7QT

Presenters:

Joy Aboim is a Technical Consultant working to help HP customers get the most from their ProLiant environments.

Jerry Walsh is a Technical Consultant, supporting UK customers with x86 virtulisation solutions.

Iain Mobberley is Consultancy Practice Leader at OCSL.

Take a look at our events page for the latest information on forthcoming hpUG events:

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

Ulink - HP-Interex EMEA Weekly E-Newsletter

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

Book Reviews on SANs and NAS and Kerberos

Book Reviews on *Using SANs and NAS* and *Kerberos - The Definitive Guide* reviewed by Steve Woltering can be found at: http://www.stats.ox.ac.uk/people/support_staff/saw/oreilly_reviews

Retrospective Book Review – The Linux Cookbook

Carla Schroder (Publisher O'Reilly, ISBN 0-596-00640-3)

Review by Steve Reece

This is a retrospective, since the book was published back in 2004 and has only just got to the top of the "I must do a review of that" pile.

That said, it's my organisation that's been the problem, not the book. Being a Cookbook from O'Reilly, it has recipes for specific problems rather than being a book that you'd sit and read to pick up the subject matter. There is an Introduction to each chapter though, so that should help the complete novice a little bit.

For someone who's grown up managing OpenVMS systems, the Linux Cookbook is helpful because it allows me to find answers to the problems that I have in moving across to a Linux system from my existing background. Most of the common issues that I experience in VMS are covered as well as the ones that I expect from a Linux text. Starting with navigating man pages (how do you spell HELP again?), the text concentrates on the "core" of Linux rather than diving off into the bells and whistles of added packages. So, CUPS, backup and remote access are covered, but using OpenOffice to create presentations and reports isn't. That's no bad thing as doing both in one text usually leads to a compromise rather than covering everything as well as I'd like. The usual suspect of Samba is an exception here, but it's largely expected as part of a Linux infrastructure, so it's no bad thing.

Having covered how to find help when you need it, Schroder progresses through the key topics of how do I edit a file, how do I start and stop the thing that I've created, before going into the more complex areas.

Both rpm-based distributions (like Red Hat) and apt-based distributions (like Debian) are covered, so it shouldn't matter which camp you're in; there should be something to help you here. The ordering is perhaps a little dangerous, since the second and third chapters discuss how to manage software products before learning anything more advanced than man pages. I've yet to find a book that covers hardening of a Linux system though – the thread is always what you shouldn't do and not what you should do. This is no exception. Maybe I've been spoiled by the security model on OpenVMS?

If you're already a sysadmin on another operating environment, The Linux Cookbook is likely to be invaluable to you for translating what you know onto Linux. If you're a complete novice sysadmin, it will help but it's still likely to be tough going.

HP Security Bulletins – HP-UX

HPSBUX02251 SSRT071449 rev.3 - HP-UX Running BIND, Remote DNS Cache Poisoning Remote DNS cache poisoning

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

CVE-2007-2926

HP-UX B.11.11, B.11.23, B.11.31 running BIND v9.2.0 or BIND v9.3.2

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 action has been taken.

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/displayProductInfo.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/displayProductInfo.do?productNumber=BIND

HP-UX B.11.31
==========
NameService.BIND-RUN
->action: install revision C.9.3.2.1.0 or subsequent URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=BIND

END AFFECTED VERSIONS

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/displayProductInfo.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 revision C.9.3.2.1.0 or subsequent

MANUAL ACTIONS: Yes - NonUpdate

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

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
Version: 3 (rev.3) - 26 November 2007 B.11.31 update 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: c01203958

Version: 1

HPSBUX02277 SSRT071453 rev.1 - HP-UX Running OpenSSL, Local Denial of Service (DoS)

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

Release Date: 2007-10-15

Last Updated: 2007-10-15

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 OpenSSL. The vulnerability could be exploited locally 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 OpenSSL before vA.00.09.07l.

BACKGROUND

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

The Hewlett-Packard Company thanks SureRun Security Team http://www.SureRun.cn 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 action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
==========
openssl.OPENSSL-CER
openssl.OPENSSL-CONF
openssl.OPENSSL-INC
openssl.OPENSSL-LIB
openssl.OPENSSL-MIS
openssl.OPENSSL-PRNG
openssl.OPENSSL-PVT
openssl.OPENSSL-RUN
action: install revision A.00.09.07l.006 or subsequent
URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I

HP-UX B.11.23
==========
openssl.OPENSSL-CER
openssl.OPENSSL-CONF
openssl.OPENSSL-INC
openssl.OPENSSL-LIB
openssl.OPENSSL-MIS
openssl.OPENSSL-PRNG
openssl.OPENSSL-PVT
openssl.OPENSSL-RUN
action: install revision A.00.09.07l.007 or subsequent
URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I

HP-UX B.11.31
==========
openssl.OPENSSL-CER
openssl.OPENSSL-CONF
openssl.OPENSSL-INC
openssl.OPENSSL-LIB

openssl.OPENSSL-MIS
openssl.OPENSSL-PRNG
openssl.OPENSSL-PVT
openssl.OPENSSL-RUN
action: install revision A.00.09.08d.003 or subsequent
URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I

END AFFECTED VERSIONS

RESOLUTION

HP has made the following available to resolve the vulnerability.

The updates are available as above

HP-UX B.11.11 (11i v1) update to OpenSSL vA.00.09.07l.006
HP-UX B.11.23 (11i v2) update to OpenSSL vA.00.09.07l.007
HP-UX B.11.31 (11i v3) update to OpenSSL vA.00.09.08d.003

MANUAL ACTIONS: Yes - Update

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) - 15 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: For further information, contact normal HP Services support channel.

HPSBUX02289 SSRT071461 rev.1 - HP-UX Running BIND 8, Remote DNS Cache Poisoning Remote DNS cache poisoning

A potential vulnerability has been identified with HP-UX running BIND 8. The vulnerability could be exploited remotely to cause DNS cache poisoning.

CVE-2007-2930

HP-UX B.11.11 running BIND v8

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 action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
==========
InternetSrvcs.INETSVCS-RUN
action: install PHNE_36185 or subsequent

END AFFECTED VERSIONS

HP has provided the following software patch to resolve the vulnerability.

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

HP-UX B.11.11 BIND 8 PHNE_36185 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) - 19 November 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: c01182588

Version: 2

HPSBUX02273 SSRT071476 rev.2 - HP-UX Running Apache, Remote Unauthorized Denial of Service (DoS)

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

Release Date: 2007-10-10

Last Updated: 2007-10-16

Potential Security Impact: Remote unauthorized 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 Apache v2.0.59.00. The vulnerability could be exploited remotely to create an unauthorized Denial of Service (DoS).

References: CVE-2007-3847, CVE-2007-3304

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP-UX B.11.11, B.11.23, B.11.31 running Apache v2.0.59.00

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 action has been taken.

AFFECTED VERSIONS

For IPv4:
HP-UX B.11.11
==========
hpuxwsAPACHE
->action: install revision A.2.0.59.00.0 or subsequent
restart Apache
URL: ftp://ssrt1476:ssrt1476@hprc.external.hp.com

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
hpuxwsAPACHE,revision=B.2.0.59.00

action: install revision B.2.0.59.00.0 or subsequent restart Apache
URL: ftp://ssrt1476:ssrt1476@hprc.external.hp.com

END AFFECTED VERSIONS

RESOLUTION

HP has made the following available to resolve the vulnerability.

OS Release Depot name MD5 Sum
B.11.11 (IPv4) HPUXWSA-B218-01-1111ipv4.depot eb3bb933baac0f05e1e0809ef1e84eb2
B.11.11 (IPv6) HPUXWSA-B218-01-1111ipv6.depot 540a56b155699336bcbfac0eaf87e3ce
B.11.23 PA-32 HPUXWSA-B218-01-1123-32.depot 2900a0cbea01b6905dc768680fbd5381
B.11.23 IA-64 HPUXWSA-B218-01-1123-64.depot 3be084d96e8a509692e37c71c0184014
B.11.31 PA-32 HPUXWSA-B218-01-1131-32.depot 861122eef70f1b53d68c5adafc64cdb5
B.11.31 IA-64 HPUXWSA-B218-01-1131-64.depot 8dc57222257fe27fb5994da16e91f9a4

The updates can be obtained from:

ftp://ssrt1476:ssrt1476@hprc.external.hp.com/

ftp://ssrt1476:ssrt1476@192.170.19.100/

MANUAL ACTIONS: Yes - Update

Install Apache v2.0.59.00.0 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) - 10 October 2007 Initial release
Revision: 2 (rev.2) - 16 October 2007 Corrected B.11.11 IPv4 version typo.

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.

HPSBUX02284 SSRT071483 rev.3 - HP-UX Running Java JRE and JDK, Remote Unauthorized Access Remote unauthorized access

Potential security vulnerabilities have been identified in Java Runtime Environment (JRE) and Java Developer Kit (JDK) running on HP-UX. These vulnerabilities may allow remote unauthorized access.

->SUN Alert ID: 103071 (CVE-2007-5240), 103072 (CVE-2007-5239), 103073 (CVE-2007-5236, CVE-2007-5237, CVE-2007-5238), 103078 (CVE-2007-5273, CVE-2007-5274), 103079 (CVE-2007-5232), 103112 (CVE-2007-5689)

->HP-UX B.11.11, B.11.23, and B.11.31 running Java Runtime Environment (JRE) v5.0.10 and earlier, and Java Developer Kit (JDK), v1.4.2.16 and earlier.

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 a fixed revision or applicable patch is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
==========
Jpi14.JPI14-COM
Jpi14.JPI14-COM-DOC
Jpi14.JPI14-IPF32
Jpi14.JPI14-PA11
Jdk14.JDK14-COM
Jdk14.JDK14-DEMO
Jdk14.JDK14-IPF32
Jdk14.JDK14-IPF64
Jdk14.JDK14-PA11
Jdk14.JDK14-PA20
Jdk14.JDK14-PA20W
Jdk14.JDK14-PNV2
Jdk14.JDK14-PWV2
Jre14.JRE14-COM
Jre14.JRE14-COM-DOC
Jre14.JRE14-IPF32
Jre14.JRE14-IPF32-HS
Jre14.JRE14-IPF64
Jre14.JRE14-IPF64-HS
Jre14.JRE14-PA11
Jre14.JRE14-PA11-HS
Jre14.JRE14-PA20
Jre14.JRE14-PA20-HS
Jre14.JRE14-PA20W
Jre14.JRE14-PA20W-HS
Jre14.JRE14-PNV2
Jre14.JRE14-PNV2-H
Jre14.JRE14-PWV2
Jre14.JRE14-PWV2-H
->action: install revision 1.4.2.17.00 or subsequent

Jdk15.JDK15-COM
Jdk15.JDK15-DEMO
Jdk15.JDK15-IPF32
Jdk15.JDK15-IPF64
Jdk15.JDK15-PA20
Jdk15.JDK15-PA20W
Jdk15.JDK15-PNV2
Jdk15.JDK15-PWV2
Jre15.JRE15-COM
Jre15.JRE15-COM-DOC
Jre15.JRE15-IPF32
Jre15.JRE15-IPF32-HS
Jre15.JRE15-IPF64
Jre15.JRE15-IPF64-HS
Jre15.JRE15-PA20
Jre15.JRE15-PA20-HS

Jre15.JRE15-PA20W
Jre15.JRE15-PA20W-HS
Jre15.JRE15-PNV2
Jre15.JRE15-PNV2-H
Jre15.JRE15-PWV2
Jre15.JRE15-PWV2-H
->action: install revision 5.0.11 or subsequent

END AFFECTED VERSIONS

HP is providing the following Java updates to resolve the vulnerabilities.
The updates are available from: http://www.hp.com/go/java

These issues are addressed in the following versions of the HP Java:

HP-UX B.11.11 JDK and JRE v5.0.11 or subsequent SDK and JRE v1.4.2.17 or subsequent
HP-UX B.11.23 JDK and JRE v5.0.11 or subsequent SDK and JRE v1.4.2.17 or subsequent
HP-UX B.11.31 JDK and JRE v5.0.11 or subsequent SDK and JRE v1.4.2.17 or subsequent

Older versions of Java may remain installed on the system or removed if no longer needed.

MANUAL ACTIONS: Yes - Update

->For Java v5.0.10 and earlier, update to Java v5.0.11 or subsequent.
->For Java v1.4.2.16 and earlier, update to Java v1.4.2.17 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) 31 October 2007 Initial release
Version: 2 (rev.2) 14 November 2007 JDK and JRE v5.0.11, SDK and JRE v1.4.2.17 are available.
Version: 3 (rev.3) 19 November 2007 Format change in references.

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.

HPSBUX02285 SSRT071484 rev.1 - HP-UX Running Aries PA Emulator, Local Unauthorized Access Local unauthorized access

Last Modified Date: Wed Oct 31 23:20:48 GMT 2007

A potential security vulnerability has been identified in the Aries PA-RISC emulation software running on HP-UX IA-64 platforms only. This vulnerability may allow local unauthorized access.

HP-UX B.11.23 (IA), and B.11.31 running all versions of Aries PA-RISC emulation software.

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 a fixed revision or applicable patch is installed.

AFFECTED VERSIONS

HP-UX B.11.23
==========
OS-Core.CORE2-64SLIB
OS-Core.CORE2-SHLIBS
action: install PHSS_35528 or subsequent

HP-UX B.11.31
==========
OS-Core.CORE2-64SLIB
OS-Core.CORE2-SHLIBS
action: install PHSS_36311 or subsequent

END AFFECTED VERSIONS

HP is providing the following patches to resolve the vulnerability.
The updates are available from: http://itrc.hp.com

HP-UX B.11.23 (IA) PHSS_35528 or subsequent
HP-UX B.11.31 PHSS_36311 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) 31 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: For further information, contact normal HP Services support channel.

HPSBUX02287 SSRT071485 rev.1 - HP-UX Running HP Secure Shell, Remotely Gain Extended Privileges Remotely gain extended privileges

A potential security vulnerability has been identified with HP-UX running HP Secure Shell. The vulnerability could be exploited remotely to gain extended privileges.

CVE-2007-4752

HP-UX B.11.11, B.11.23, and B.11.31 running HP Secure Shell

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
==========
Secure_Shell.SECURE_SHELL
action: install revision A.04.70.003 or subsequent URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

HP-UX B.11.23
==========
Secure_Shell.SECURE_SHELL
action: install revision A.04.70.004 or subsequent URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

HP-UX B.11.31
==========
Secure_Shell.SECURE_SHELL
action: install revision A.04.70.005 or subsequent URL:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

END AFFECTED VERSIONS

HP has provided the following software updates to resolve this vulnerability.

The updates are available for download as above.

OS Release HP Secure Shell Version

HP-UX B.11.11 (11i v1) A.04.70.003 or subsequent
HP-UX B.11.23 (11i v2) A.04.70.004 or subsequent
HP-UX B.11.31 (11i v3) A.04.70.005 or subsequent

MANUAL ACTIONS: Yes - Update

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) - 07 November 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.

HPSBUX02292 SSRT071499 rev.1 - HP-UX Running Apache, Remote Execution of Arbitrary Code

A potential security vulnerability has been identified with HP-UX Apache. The vulnerability could be exploited remotely to execute arbitrary code.

CVE-2007-5135

HP-UX B.11.11, B.11.23, B.11.31 running Apache v2.0.59.00.0 or earlier.

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 action has been taken.

AFFECTED VERSIONS

For IPv4:
HP-UX B.11.11
==========
hpuxwsAPACHE
action: install revision A.2.0.59.00.1 or subsequent restart Apache
URL: ftp://srt1499:srt1499@hprc.external.hp.com

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
hpuxwsAPACHE,revision=B.2.0.59.00
hpuxwsAPACHE,revision=B.2.0.59.00.0
action: install revision B.2.0.59.00.1 or subsequent restart Apache
URL: ftp://srt1499:srt1499@hprc.external.hp.com

END AFFECTED VERSIONS

HP has provided the following software updates to resolve this vulnerability.

The updates are available for download from:

ftp://srt1499:srt1499@hprc.external.hp.com/
ftp://srt1499:srt1499@192.170.19.100/

OS Release Depot name MD5 Sum
B.11.11 (IPv4) HPUXWSA-B218-02-1111ipv4.depot 2306e1580461411fb743d0d74e4a44bc
B.11.11 (IPv6) HPUXWSA-B218-02-1111ipv6.depot 4740ab73eda685603748f4cbe24f3440
B.11.23 PA-32 HPUXWSA-B218-02-1123-32.depot 78561137e265c9f23aba4e4d832e4de6
B.11.23 IA-64 HPUXWSA-B218-02-1123-64.depot 809d8c3b99942359bdcb526235e1cf6b
B.11.31 PA-32 HPUXWSA-B218-02-1131-32.depot 39a5d364a387a89ea6f632cfc1b0eafa
B.11.31 IA-64 HPUXWSA-B218-02-1131-64.depot faa16d98407b49b5490428b0e2c1e09a

MANUAL ACTIONS: Yes - Update
Install Apache v2.0.59.00.1 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) - 28 November 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.

HP Security Bulletins - Storage Management Appliance - Microsoft

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01208742

Version: 1

HPSBST02280 SSRT071480 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-055 to MS07-060

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

Release Date: 2007-10-15

Last Updated: 2007-10-15

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: MS07-055, MS07-056, MS07-057, MS07-058, MS07-059, MS07-060.

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

MS07-055
Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-056
Security Update for Outlook Express and Windows Mail (941202) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-057
Cumulative Security Update for Internet Explorer (939653) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-058
Vulnerability in RPC Could Allow Denial of Service (DoS) (933729) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-059
Vulnerability in Windows SharePoint Services 3.0 and Office SharePoint Server 2007 Could Result in Elevation of Privilege Within the SharePoint Site (942017) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-060
Vulnerability in Microsoft Word Could Allow Remote Code Execution (942695) 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

PRODUCT SPECIFIC INFORMATION

HISTORY

Version: 1 (rev.1) - 15 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: For further information, contact normal HP Services support channel.

HPSBST02291 SSRT071498 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-061 and MS07-062 - Please check the table below

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.

MS07-061, MS07-062.

Storage Management Appliance v2.1 Software running on:

Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

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.

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
MS07-061
Vulnerability in Windows URI Handling Could Allow Remote Code Execution
(943460) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

MS07-062
Vulnerability in DNS Could Allow Spoofing (941672) 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) - 21 November 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.

HP Security Bulletin – Java Runtime Environment Proxy and JVM

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01180021

Version: 1

HPSBGN02270 SSRT0822 rev.1 - Re-release of HPSBMI01199 Java Runtime Environment Proxy and JVM, Remote Increased Privilege, Unauthorized Access

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

Release Date: 2002-07-16

Last Updated: 2007-10-02

Potential Security Impact: Remote increased privilege or unauthorized access

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

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with Java JRE and JVM. This vulnerability could be exploited by a remote user to gain increased privilege or unauthorized access.

References: SUN Bulletin #00216 & #00218, CAN-2002-0058, CAN-2002-0076, HPSBMI01199

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Product Impacted Version(s)

Management Software Compaq Insight Manager 7, Compaq Insight Manager XE, the Compaq Management Agents and the Remote Insight Lights-Out Edition Card leverage Java technology to deliver portions of their functionality. The Java software causing this problem is delivered as part of the Java Runtime Environment used to enable access to these management products and as part of the server-side software embedded in Compaq Insight Manager XE and Compaq Insight Manager 7.

Insight Manager XE - Insight Manager XE uses the Microsoft Java Runtime Environment integrated into Microsoft Internet Explorer.

Insight Manager 7 - Insight Manager 7 uses the Sun Java Runtime Environment version 1.3.1 in place of the Microsoft Java Runtime Environment.

Management Agents See Resolution Table

Remote Insight Lights-Out Edition / Integrated Lights-Out on ProLiant DL360 G2 See Resolution Table HP Tru64 UNIX V4.0f SDK and JRE 1.1.7B-2 V4.0g SDK and JRE 1.1.7B-2 V5.0a SDK and JRE 1.1.7B-6 V5.1 SDK and JRE 1.1.8-6 (default for tools) and 1.2.2-6 V5.1a SDK and JRE 1.1.8-13 default for tools (includes fix for proxy #0216) and 1.2.2-8

HP Nonstop Himalaya No applets run on the Compaq NonStop Himalaya operating systems. This is not a vulnerability on these systems.

HP OpenVMS

*Please note that this is an issue for the Alpha architecture only.
OpenVMS on Vax does not support Java. V7.2, V7.2-1, V7.2-1h1, V7.2-1h2, V7.2-2 SDK and JRE 1.1.6-2 V7.3 SDK and JRE 1.1.8-5

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI01199 SSRT0822 rev.0.

RESOLUTION

The following table outlines the suggested resolutions to the vulnerabilities described above. Suggested remedies will be different on a product-by-product depending on developer of the Java Runtime Environment and any dependencies for synchronization between server and client side components.

Product Recommendation

Insight Manager XE - Insight Manager XE uses the Microsoft Java Runtime Environment integrated into Microsoft Internet Explorer. HP recommends that Insight Manager XE users upgrade to Insight Manager 7 SP1 that will be available for download in the first half of May at http://www.compaq.com/manage

Insight Manager 7 SP1 leverages version 1.3.1_02 of the Sun Java Runtime Environment that addresses the vulnerabilities described above. Prior to the release of Insight Manager 7 SP1, HP recommends that users exercise care when browsing to sites outside of the internal network using a browser with a vulnerable version of the Microsoft Java Runtime Environment.

While it is possible to update the browser to the version of the Java Runtime Environment recommended by Microsoft, this version has not been tested with Insight Manager XE and HP cannot guarantee that Insight Manager XE will function properly.

Insight Manager 7 - Insight Manager 7 uses the Sun Java Runtime Environment version 1.3.1 in place of the Microsoft Java Runtime Environment. HP is in the process of incorporating version 1.3.1_02 of the runtime environment, which fixes the aforementioned vulnerability, into Insight Manager 7 Service Pack 1.

Insight Manager 7 SP1 will be available at the beginning of May. Users may not use version 1.3.1_02 of the plug-in with the current version of Insight Manager 7 as newer versions of the Sun Java Runtime Environment are not backwards compatible and the Insight Manager 7 may not function properly if client and server side runtime environments are not of the same version.

HP recommends that current Insight Manager 7 users close Microsoft Internet Explorer prior to browsing to untrusted sites outside of the corporate firewall. This will ensure that the Java plug-in is closed prior to browsing to sites on the public Internet. With Insight Manager 7 SP1, the requirement to close the browser prior to visiting public sites will be removed.

Management Agents Update to the version of the Java Runtime Environment that Microsoft Recommends. This information may be found at http://www.microsoft.com/java/vm/dl_vm40.htm

Remote Insight Lights-Out Edition / Integrated Lights-Out on ProLiant DL360 G2 Update to the Java(TM) 2 Runtime Environment, Standard Edition, version 1.3.1_02 http://java.sun.com/j2se/1.3/download.html

To download this software simply click on the hyperlink.

HP Tru64 UNIX

V4.0f SDK and JRE 1.1.7B-2
V4.0g SDK and JRE 1.1.7B-2
V5.0a SDK and JRE 1.1.7B-6
V5.1 SDK and JRE 1.1.8-6 (default) and 1.2.2-6
V5.1a SDK and JRE 1.1.8-10 (default includes proxy fix) and 1.2.2-8

HP Tru64 UNIX V4.0f - update to Java 1.1.7B-10
HP Tru64 UNIX V4.0g - update to Java 1.1.8-14 (includes proxy fix)
HP Tru64 UNIX V5.0a update default to Java 1.1.8-14 and update to Java 1.3.1-3 (includes fixes)
HP Tru64 UNIX V5.1 - update default to 1.1.8-14 (includes fixes) and update Java 1.2.2-8 to Java 1.3.1-3 (includes fixes)
HP Tru64 UNIX V5.1a - update default to 1.1.8-14 (includes fixes) and update Java 1.2.2-8 to Java 1.3.1-3 (includes fixes)
HP Tru64 UNIX 5.0 and higher include some Java-based tools that depend on the Java environment default version that ships with the operating system and is installed in /usr/bin. If changing the default system Java environment version to any release after Java 1.1.8, some operating system tools, such as the SysMan Station, the SysMan Station authentication daemon, and the Logical Storage Manager (LSM) Storage Administrator, will not work correctly.

If problems are experienced maintaining the default installation for HP

Tru64 V5.0 or later, please contact normal HP Tru64 support channels for assistance.

HP OpenVMS

V7.2 V7.2-1 V7.2-1h1, V7.2-1h2, V7.2-2 SDK & JRE 1.1.6-2
V7.3 SDK & JRE 1.1.8-5

The following table shows Java versions that are available at http://www.compaq.com/java/alpha and indicates if the version includes the fix:

HP OpenVMS - Java 1.3.0-2 (includes proxy fix only)

Update to: Java 1.3.1-3 (includes fixes)

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN

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 Tru64 UNIX Running Apache Tomcat

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01192554

Version: 1

HPSBTU02276 SSRT071472 rev.1 - HP Tru64 UNIX Running Apache Tomcat, Remote Unauthorized Access, Remote Denial of Service (DoS)

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

Release Date: 2007-10-15

Last Updated: 2007-10-15

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

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

VULNERABILITY SUMMARY

Potential vulnerabilities have been identified with HP Tru64 UNIX Running Apache Tomcat. The vulnerabilities could be exploited to allow remote unauthorized access or remote Denial of Service (DoS).

References: CVE-2007-3382, CVE-2007-3385, CVE-2007-3386

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Tru64 UNIX running Tomcat v5.5.10 (supplied by Internet Express v6.5)

Tru64 UNIX running Tomcat v5.5.17 (supplied by Internet Express v6.6)
Tru64 UNIX running Tomcat v5.5.23 (supplied by Internet Express v6.7)

BACKGROUND

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

RESOLUTION

HP has provided the following Early Release Patch (ERP) kit to resolve these vulnerabilities.

Early Release Patch for Internet Express v6.5, v6.6, v6.7

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64V51B-IX671-TOMCAT5525-SSRT147-20071003

Name: T64V51B-IX671-TOMCAT5525-SSRT147-20071003.tar.gz
MD5 Checksum: f5219a90e45abe949aebaedcbb43c680

Note: The kit distributes Tomcat v5.5.25 (setld file), the Tomcat v5.5.25 sources, and the license agreement.

HISTORY

Version: 1 (rev.1) 15 October 2007 Initial release

Support: For further information, contact normal HP Services support channel.

HP Security Bulletins - HP Tru64 and OpenVMS

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01180076

Version: 1

HPSBGN02271 SSRT2253 rev.1 - Re-release of HPSBMI01201 HP Tru64 UNIX & HP OpenVMS running Secure Web Server, Remote Arbitrary Code Execution or Denial of Service (DoS)

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

Release Date: 2002-06-30

Last Updated: 2007-10-02

Potential Security Impact: Arbitrary code execution or denial of service (DoS)

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

VULNERABILITY SUMMARY

A potential vulnerability has been identified with Compaq's Secure Web Server (CSWS) for HP Tru64 UNIX and HP OpenVMS where remote users may execute arbitrary code or create a denial of service (DoS).

References: CAN-2002-0392, CERT CA-2002-17, HPSBMI01201

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
CSWS for HP Tru64 UNIX
CSWS V5.8.1 and earlier Internet Express V5.9
CSWS Internet Express EAK V2.0

CSWS for HP OpenVMS
HP OpenVMS CSWS 1.0-1
HP OpenVMS CSWS 1.1-1
HP OpenVMS CSWS 1.2

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI01201 SSRT2253 rev.0.

RESOLUTION

HP has made the following software updates available to resolve the vulnerability.

HP Tru64 UNIX for V5.0a or later:

A Compaq Secure Web Server security update kit is available for download at:
http://tru64unix.compaq.com/internet/download.htm#sws_v591

Select and install the CSWS (Compaq Secure Web Server) kit V5.9.1

Installed Version Install Updated Server Kit CSWS V5.8.2 and earlier CSWS V5.9.1

HP Tru64 UNIX INTERNET EXPRESS V5.9

SECURE WEB SERVER: Internet Express for Tru64 also contains the Secure Web Server. All versions of Internet Express up to and including version 5.9 are affected if the IAEAPCH* subset is installed. Internet Express V5.9 is currently in manufacturing and is scheduled to begin shipping.

For all versions of Internet Express, obtain the Secure Web Server for HP Tru64 from the download site and only install the IAEAPCH591 subset (the Secure Web Server subset).

Note: When installing Internet Express version 5.9, the IAEAPCH591 subset will need to be uninstalled, and then reinstalled after the installation of the desired Internet Express subsets (this is mandated by version checking in many of the web related subsets).

Apache 2.0 Early Adopters Kit (2.0.39 beta): All versions are affected prior to version 5.0 (Apache 2.0.39). The latest version of the EAK may be downloaded from:
http://www.tru64unix.compaq.com/internet/download.htm

CSWS for HP OpenVMS V7.1-2 or later: A Compaq Secure Web Server security update kit is available for download at:
http://www.openvms.compaq.com/openvms/products/ips/apache/csws_patches.html

Installed Version Update Kit
CSWS V1.2 CSWS12_UPDATE V3.0
CSWS V1.1-1 CSWS111_UPDATE V2.0
CSWS V1.0-1 CSWS101_UPDATE V2.0

After completing the update, Compaq strongly recommends that you perform an immediate backup of your system disk so that any subsequent restore operations begin with updated software. Otherwise, you must reapply the patch after a future restore operation.

Note: if at some future time upgrade of the system is anticipated to a later patch version, re-application of the appropriate patch will be necessary.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN

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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179943

Version: 1

HPSBGN02269 SSRT2310a rev.1 - Re-release of HPSBMI01195 Tru64 and OpenVMS Using OpenSSL, Multiple Remotely Exploitable Vulnerabilities

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

Release Date: 2002-09-27

Last Updated: 2007-10-02

Potential Security Impact: Multiple remotely exploitable vulnerabilities

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

VULNERABILITY SUMMARY

Multiple remotely exploitable vulnerabilities have been recently discovered with OpenSSL by many security research groups and reported in an advisory by CERT/CC CA-2002-23and CERT IN-2002-04.

This bulletin is in follow-up to the previous announcements that describe this potential threat that impact HP Tru64 UNIX and HP OpenVMS.

References: CERT CA-2002-23, CAN-2002-0655, CAN-2002-0656, CAN-2002-0657, CAN-2002-0659, HPSBMI01195

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP OpenVMS

HP OpenSSL for HP OpenVMS Alpha V1.0

HP V5.3 TCP/IP Services for OpenVMS

HP OpenVMS Secure Web Server v1.1-1, v1.2

HP Tru64 UNIX

Internet Express V5.9 for Tru64 UNIX Secure Web Server & Internet Express EAK V2.0

HP Tru64 UNIX Secure Web Server V5.8.1 and earlier

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
RESOLUTION

HP OpenVMS

OpenSSL for OpenVMS Alpha V1.0

OpenVMS engineering has released a new version of Compaq SSL for OpenVMS Alpha, Version 1.0-A that corrects the security vulnerabilities highlighted in CERT advisory CA-2002-23 for all ports of OpenSSL.

To download OpenSSL for OpenVMS Alpha V1.0-A go to the following website:
http://www.openvms.compaq.com/openvms/products/ssl/ssl.html

NOTE: Customers who have already installed OpenSSL for OpenVMS Alpha V1.0 should remove it with the following command $ PRODUCT REMOVE SSL and install V1.0-a

V5.3 TCP/IP services for OpenVMS

V5.3 TCP/IP services for OpenVMS is susceptible to the Buffer overflow conditions in the BIND 9 Server & utilities on Alpha only. Customers are asked not to use any keying mechanisms (including tsig and dnssec) which is done by editing the BIND configuration file TCPIP$BIND.CONF, until a patch is provided.

UPDATE: 17 Sep., 2002 - This issue has been resolved with the release of Compaq TCP/IP Services for OpenVMS V5.3 ECO 1 for V7.2 VAX, V7.2-2, V7.3 & V7.3-1 ALPHA

Compaq TCP/IP VAXVMS-TCPIP_ECO-V0503-181-4 Compaq TCP/IP Services for OpenVMS V5.3 ECO Summary Note: Please review the README file(s) for this patch prior to installation.

For OpenVMS Alpha use:

http://ftp1.support.compaq.com/patches/public/vms/axp/v7.3/tcpip/5.3/

for OpenVMS Vax use:

http://ftp1.support.compaq.com/patches/public/vms/vax/v7.3/tcpip/5.3/

Secure Web Server V1.1-1 - Secure Web Server is only vulnerable to the SSLv2 buffer-overflow vulnerability VU#102795. HP has released security update kits for SWS 1.1-1 and CSWS 1.2.

SWS V1.2: Install SWS12_UPDATE V4.0

http://www.openvms.compaq.com/openvms/products/ips/apache/csws_patches.html

SWS V1.1-1: Install SWS111_UPDATE V3.0
http://www.openvms.compaq.com/openvms/products/ips/apache/csws_patches.html

HP Tru64 UNIX

Internet Express Secure Web Server V5.8.1 - Update to Secure Web Server 5.9.2 (Apache)
http://tru64unix.compaq.com/internet/register_sws.html

Note: The kit requires HP Tru64 UNIX V5.0A or later. * If SSL has been enabled for anything from the Internet Express distribution other than Secure Web Server, please contact your normal HP Services Support channel. Before installing the software, review the Secure Web Server RELEASE NOTES for important information about this release.

Internet Express EAK V2.0 Update to Apache 2.0 Early Adopters Kit (2.0.39)

Note: The kit requires HP Tru64 UNIX V5.1 or later.
http://tru64unix.compaq.com/internet/register_apache.html

Before installing the software, review the Secure Web Server RELEASE NOTES for important information about this release.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN

Support: For further information, contact normal HP Services support channel.

HP Security Bulletin - HP System Management Homepage

HPSBMA02274 SSRT071445 rev.2 - 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: 2007-10-17

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) revision A.2.2.6.2 or earlier 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 revision A.2.2.6.2 or subsequent and install
->PHSS_36869 or subsequent

HP-UX B.11.23
==========
SysMgmtHomepage.SMH-RUN
->action: install revision A.2.2.6.2 or subsequent and install
->PHSS_36870 or subsequent

HP-UX B.11.31
==========
SysMgmtHomepage.SMH-RUN
->action: install revision A.2.2.6.2 or subsequent and install PHSS_36871 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has provided patches to resolve these vulnerabilities. The patches are available from http://itrc.hp.com

-> Note: The patches listed above are for SMH vA.2.2.6.2 only. Systems running SMH prior to v.A.2.2.6.2 must be updated to SMH vA.2.2.6.2 and then the appropriate patch must be installed. SMH versions after vA.2.2.6.2, when available, will resolve the vulnerability and will not require not require the patches listed above.

->SMH vA.2.2.6.2 or subsequent is available from:
http://www.hp.com/go/softwaredepot/

MANUAL ACTIONS: Yes - Update
->Update to SMH vA.2.2.6.2 or subsequent. Install patches on SMH v.A.2.2.6.2.

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
Version:2 (rev.2) - 17 October 2007 Patches require update to SMH vA.2.2.6.2

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 Select Identity

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01081130

Version: 1

HPSBMA02230 SSRT071436 rev.2 - HP Select Identity, Remote Unauthorized Access

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

Release Date: 2007-10-10

Last Updated: 2007-10-15

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 HP Select Identity. The vulnerability could be exploited to allow remote unauthorized access.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP Select Identity v4.01 prior to v4.01.011 and v4.1x prior to v4.13.002 running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX.

BACKGROUND

For a PGP signed version of this security bulletin please write to:

security-alert@hp.com

RESOLUTION

HP has provided the following software patches to resolve the vulnerability. Please contact HP Support to receive the patches.

->HP Select Identity v4.01 running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX v4.01.011 patch

->HP Select Identity v4.1x running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX v4.13.002 patch

Note: After the patch is installed, the passwords for the application server and database must be changed.

HISTORY

Version: 1 (rev.1) - 10 October 2007 Initial release
Version: 2 (rev.2) - 15 October 2007 Correct product name in Resolution

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.

HPSBMA02293 SSRT071494 rev.1 - HP Select Identity, Remote Unauthorized Access
Document ID: emr_na-c01293337-1

Last Modified Date: Mon Dec 03 22:22:03 GMT 2007

Submitted Date: Thu Nov 29 22:35:56 GMT 2007

HPSBMA02293 SSRT071494 rev.1 - HP Select Identity, Remote Unauthorized Access Remote unauthorized access

A potential security vulnerability has been identified with HP Select Identity. The vulnerability could be exploited remotely to gain unauthorized access.

CVE-2007-6194

HP Select Identity v4.01 prior to v4.01.012 and v4.1x prior to v4.13.003 running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX.

HP has provided the following software patches to resolve the vulnerability. Please contact normal HP Services support channels to receive the patches.

HP Select Identity v4.01 running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX v4.01.012 patch
HP Select Identity v4.1x running on Windows 2003 Server, Red Hat Linux AS3, Solaris, and HP-UX v4.13.003 patch

HISTORY

Version: 1 (rev.1) - 3 December 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.

HP Security Bulletins - ProCurve

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179933

Version: 1

HPSBGN02267 SSRT3647 rev.1 - Re-release of HPSBMI00006 ProCurve 5300 Switches, Remote Denial of Service (DoS)

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

Release Date: 2003-11-24

Last Updated: 2007-10-02

Potential Security Impact: Remote denial of service (DoS)

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

VULNERABILITY SUMMARY

A vulnerability in ProCurve 5300 series switches may allow creation of a remote denial of service (DoS).

References: HPSBMI00006

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP ProCurve Switch 5304XL (J4850A), 5348XL (J4849A), 5372XL (J4848A), 5308XL (J4819A).

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI0311-006 SSRT3647 rev.0.

The HP ProCurve Switches potentially suffer an adverse reaction to the presence of the Blaster/Welchia worms. Networking performance deteriorates resulting in the appearance of a Denial of Service for connected end nodes, generally running Microsoft Windows operating systems. HP ProCurve Switches can exhibit deteriorating performance and fail to function in presence of RPC worms such as Welchia and Blaster.

Only the following HP ProCurve Switches are affected: 5304XL (J4850A), 5348XL (J4849A), 5372XL (J4848A), 5308XL (J4819A).

NOTE: This problem does not directly impact HP-UX, MPE/iX, HP NonStop Servers, HP OpenVMS, nor HP Tru64 UNIX/Trucluster Server.

RESOLUTION

HP has made the following software updates available to resolve the vulnerability.

The software updates are available from:
http://www.hp.com/rnd/software/switches.htm

ProCurve 5300 series switches Install firmware E.07.40, or subsequent

Several steps need to be taken to mitigate the problem.

1. Locate and remove worms from infected and connected network clients.
To accomplish that task, download the Snort* utility which is designed to identify a network client infected by the Blaster and/or Welchia worms. http://www.snort.org/

Follow the recommended instructions provided to install and to locate and remove these worms from a network.

The following link provides some details of how to detect traffic that is caused by such worms and the data from this link can be used to compare to the traces that captured from a network.
http://www.symantec.com

2. Administrators should take actions to prevent worm infiltrations on the network by ensuing that the latest patches for security vulnerabilities are applied to end clients via Microsoft Security releases.
http://update.microsoft.com

3. Download and install the new switch software version E.07.40 or subsequent from:
http://www.hp.com/rnd/software/switches.htm

If further assistance is required, contact a local ProCurve Customer Care Center, or visit the web site at:
https://my.procurve.com/help/help_topics.aspx?CultureCode=en-US

* Snort is not included with HP Operating Systems and is not supported by HP; the information has been included in this document as a reference to customers who may be interested in evaluating it as it applies to this particular subject.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change MI to GN.

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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179938

Version: 1

HPSBGN02268 SSRT4696 rev.1 - Re-release of HPSBMI01041 HP ProCurve Routing Switches, TCP Remote Denial of Service (DoS)

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

Release Date: 2004-05-18

Last Updated: 2007-10-02

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 ProCurve Routing Switches running TCP which could be exploited to cause a remotely exploitable Denial of Service (DoS).

References: NISCC 236929, CVE CAN-2004-0230, CERT TA04-111A, HPSBMI01041

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP ProCurve Routing Switch 9315M, 9308M, 9304M and all managed HP EtherTwist, HP AdvanceStack and HP ProCurve devices.

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This information is applicable for the following security vulnerability alerts:

NISCC Vulnerability Advisory 236929 - Vulnerability Issues in TCP

US-CERT Technical Cyber Security Alert TA04-111A Vulnerabilities in TCP

CVE name CAN-2004-0230

The industry standard TCP specification (RFC793) has a vulnerability whereby established TCP connections can be reset by an attacker. The TCP stack that is part of the software used in managed HP EtherTwist, HP AdvanceStack and HP ProCurve devices is in conformance with this specification, and therefore contains this potential vulnerability. The TCP connections that are affected due to this situation are only those terminating on these devices, not those passing through these devices.

HP ProCurve Routing Switch 9315M, 9308M, and 9304M which have BGP functionality can experience a Denial of Service, the duration of which would be the time needed by the device to rebuild routing tables.

TCP sessions, including Telnet, SSH, SFTP and HTTP on all managed HP EtherTwist, HP AdvanceStack and HP ProCurve devices may be disconnected without warning. TCP sessions that have been disconnected can be re-established.

TCP sessions, including Telnet, SSH, SFTP and HTTP on all managed HP EtherTwist, HP AdvanceStack and HP ProCurve devices may be disconnected without warning. TCP sessions that have been disconnected can be re-established.

RESOLUTION

For the HP ProCurve Routing Switch 9315M, 9308M, and 9304M, the BGP technology can be protected by using the MD5 hash protection feature. HP recommends that our BGP customers implement MD5 protection as soon as possible to protect their connections against this type of attack.

Other managed HP EtherTwist, HP AdvanceStack and HP ProCurve devices are generally not impacted as TCP sessions that were disconnected can be re-established.

As a good practice, HP recommends the appropriate inactivity timeout feature on the device for each type of TCP session be implemented. TCP sessions include Telnet, SSH, SFTP and HTTP

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN

Support: For further information, contact normal HP Services support channel.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179860

Version: 1

HPSBGN02272 SSRT071396 rev.1 - Re-release of HPSBMI02210 ProCurve Series 9300m Switches, Remote Denial of Service (DoS)

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

Release Date: 2007-05-09

Last Updated: 2007-10-02

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 in the ProCurve Series 9300m Switches. The vulnerability could be remotely exploited resulting in a Denial of Service (DoS).

References: HPSBMI02210

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. ProCurve Series 9300m Switches - system software versions 08.0.01c - 08.0.01j

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
RESOLUTION

-> Customers who have installed the vulnerable system software versions 08.0.01c - 08.0.01j should install 08.0.01k.

-> The version 08.0.01k software can be obtained from the Procurve Networking Software for Switches website: http://www.hp.com/rnd/software/switches.htm

HISTORY:

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN

Support: For further information, contact normal HP Services support channel.

HP Security Bulletins - OpenView

HPSBMA02288 SSRT071465 rev.1 - HP OpenView Operations (OVO) Running on HP-UX and Solaris, Remote Unauthorized Access, Denial of Service (DoS) Remote unauthorized access, Denial of Service (DoS)

Potential security vulnerabilities have been identified in OpenView Operations (OVO) running on HP-UX and Solaris. These vulnerabilities may be exploited remotely to gain unauthorized access or to create a Denial of Service (DoS).

SUN Alert 102995, 102997, CVE-2007-3922, CVE-2007-3698

HP OpenView Operations(OVO) 7.1X and 8.X running on HP-UX B.11.11, B.11.23, B.11.31, and Solaris.

Note: The following is for use by the HP-UX Software Assistant. Only the HP-UX versions are listed.

AFFECTED VERSIONS

For OVO 7.1X

HP-UX B.11.11
==========
OVOPC-WWW.OVOPC-WWW-GUI
action: install PHSS_37197 or subsequent

For OVO 8.X

HP-UX B.11.11
HP-UX B.11.23 (PA)
==========
OVOPC-WWW.OVOPC-WWW-GUI
action: install PHSS_37183 or subsequent

HP-UX B.11.23 (IA)
HP-UX B.11.31
==========
OVOPC-WWW.OVOPC-WWW-GUI
action: install PHSS_37182 or subsequent

END AFFECTED VERSIONS

HP has provided the following patches to resolve the vulnerabilities.
The patches can be downloaded from http://support.openview.hp.com/patches/

OVO 7.1X HP-UX B.11.11 PHSS_37197 or subsequent
OVO 7.1X Solaris ITOSOL_00619 or subsequent
OVO 8.X HP-UX B.11.11 PHSS_37183 or subsequent
OVO 8.X HP-UX B.11.23 (PA) PHSS_37183 or subsequent
OVO 8.X HP-UX B.11.23 (IA) PHSS_37182 or subsequent
OVO 8.X HP-UX B.11.31 PHSS_37182 or subsequent
OVO 8.X Solaris ITOSOL_00618 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) - 13 November 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: c00727143

Version: 6

HPSBMA02133 SSRT061201 rev.6 - 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: 2007-10-24

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 - October 2007

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

->Oracle for OpenView (OfO) v8.1.7, v9.1.01, v9.2, v9.2.0, v10g, v10gR2 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 - October 2007.

For more information:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.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:

ORA200BC OfO v8.1.7 for HP-UX LTU ORA205BC OfO v8.1.7 for HP-UX 5 LTU Bundle ORA230BC OfO v8.1.7 for HP-UX Media ORA240BC OfO v8.1.7 for HP-UX Eval LTU & Media ORA300BC OfO v8.1.7 for Win 2000/NT LTU ORA305BC OfO v8.1.7 for Win 2000/NT 5 LTU Bundle ORA330BC OfO v8.1.7 for Win 2000/NT Media ORA340BC OfO v8.1.7 for Win 2000/NT Eval LTU ORA400BC OfO v8.1.7 for Sun Solaris LTU ORA405BC OfO v8.1.7 for Sun Solaris 5 LTU Bundle ORA430BC OfO v8.1.7 for Sun Solaris Media ORA440BC OfO v8.1.7 for Sun Solaris Eval LTU ORA600CA OfO for Linux LTU ORA605CA OfO for Linux LTU Service Bureaus Bundle ORA631EE Oracle EE v9.2 HP-UX - 1 CPU LTU ORA631SE Oracle SE 9v.2 HP-UX - 1 CPU LTU ORA230CA OfO v9.2 64bit HP-UX 11&11.11 Media Kit ORA643EE Oracle EE v9.2 Windows - 1 CPU LTU ORA643SE Oracle SE v9.2 Windows - 1 CPU LTU ORA330CA OfO v9.2 32bit Windows Media Kit ORA637EE Oracle EE v9.2 Solaris 64 - 1 CPU LTU ORA634SE Oracle SE v9.2 Solaris 32 - 1 CPU LTU ORA637SE Oracle SE v9.2 Solaris 64 - 1 CPU LTU ORA430CA OfO v9.2 32bit Sun Solaris 2.7&2.8 Media ORA431CA OfO v9.2 64bit Sun Solaris 2.7&2.8 Media ORA646EE Oracle EE v9.2 Tru64 - 1 CPU LTU ORA646SE Oracle SE v9.2 Tru64 - 1 CPU LTU ORA530CA OfO v9.1.01 64bit Tru64 V5.1a Media Kit ORA640EE Oracle EE v9.2 Linux - 1 CPU LTU ORA640SE Oracle SE v9.2 Linux - 1 CPU LTU ORA630CA OfO v9.2.0 for Linux Media Kit T2607AA Oracle for OpenView Partition Opt LTU T3847EE Oracle v10g EE HP-UX , 1 CPU LTU T3847SE Oracle v10g SE HP-UX , 1 CPU LTU T3848AA Oracle v10g EE/SE HP-UX PA-RISC 64, Media T3847AA Oracle v10g EE/SE HP-UX Itanium, Media T3843EE Oracle v10g EE Windows 32, 1 CPU LTU T3843SE Oracle v10g SE Windows 32, 1 CPU LTU T3843AA Oracle v10g EE/SE Windows 32, Media T3844EE Oracle v10g EE Solaris 64, 1 CPU LTU T3844SE Oracle v10g SE Solaris 64, 1 CPU LTU T3844SE Oracle v10g SE Solaris 64, 1 CPU LTU T3844AA Oracle v10g EE/SE Solaris 64, Media T3844AA Oracle v10g EE/SE Solaris 64, Media T3849EE Oracle v10g EE Tru64, 1 CPU LTU T3849SE Oracle v10g SE Tru64, 1 CPU LTU T3849AA Oracle v10g EE/SE Tru64, Media T3845EE Oracle v10g EE Linux, 1 CPU LTU T3845SE Oracle v10g SE Linux, 1 CPU LTU T3846AA Oracle v10g EE/SE Linux x86-32, Media T3845AA Oracle v10g EE/SE Linux x86-64, Media T4855EE Oracle v10gR2 EE HP-UX , 1 CPU LTU T4855AA Oracle v10gR2 EE/SE HP-UX PA-RISC 64, Media T4856AA Oracle v10gR2 EE/SE HP-UX Itanium, Media T4857EE Oracle v10gR2 EE Windows 32, 1 CPU LTU T4857SE Oracle v10gR2 SE Windows 32, 1 CPU LTU

T4857AA Oracle v10gR2 EE/SE Windows 32, Media T4858EE Oracle v10gR2 EE Solaris 64, 1 CPU LTU T4858SE Oracle v10gR2 SE Solaris 64, 1 CPU LTU T4858SE Oracle v10gR2 SE Solaris 64, 1 CPU LTU T4858AA Oracle v10gR2 EE/SE Solaris 64, Media T4858AA Oracle v10gR2 EE/SE Solaris 64, Media T4860EE Oracle v10gR2 EE Linux, 1 CPU LTU T4860SE Oracle v10gR2 SE Linux, 1 CPU LTU T4860AA Oracle v10gR2 EE/SE Linux x86-32, Media ORA200CA OfO v9.2 64bit HP-UX 11&11.11 LTU ORA205CA OfO v9.2 64bit HP-UX 11&11.11 5 LTUs ORA230CA OfO v9.2 64bit HP-UX 11&11.11 Media Kit ORA300CA OfO v9.2 32bit Windows LTU ORA305CA OfO v9.2 32bit Windows 5 LTUs ORA330CA OfO v9.2 32bit Windows Media Kit ORA400CA OfO v9.2 32bit Sun Solaris 2.7&2.8 LTU ORA401CA OfO v9.2 64bit Sun Solaris 2.7&2.8 LTU 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 ORA430CA OfO v9.2 32bit Sun Solaris 2.7&2.8 Media ORA431CA OfO v9.2 64bit Sun Solaris 2.7&2.8 Media 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 Oracle for OpenView for Linux LTU ORA605CA OfO for Linux LTU Service Bureaus Bundle ORA630CA OfO v9.2.0 for Linux Media Kit T3848AA Oracle v10g EE/SE HP-UX PA-RISC 64, Media T3847AA Oracle v10g EE/SE HP-UX Itanium, Media T3843AA Oracle v10g EE/SE Windows 32, Media T3844AA Oracle v10g EE/SE Solaris 64, Media T3844AA Oracle v10g EE/SE Solaris 64, Media T3849AA Oracle v10g EE/SE Tru64, Media T3846AA Oracle v10g EE/SE Linux x86-32, Media T3845AA Oracle v10g EE/SE Linux x86-64, Media T4862AA Oracle v10g R2 EE HP-UX 1-Sys LTU T4863AA Oracle v10g R2 EE HP-UX 5-Sys LTU T4864AA Oracle v10g R2 EE HP-UX Itanium 1-Sys LTU T4865AA Oracle v10g R2 EE HP-UX Itanium 5-Sys LTU T4866AA Oracle v10g R2 EE Windows 1-Sys LTU T4867AA Oracle v10g R2 EE Solaris 1-Sys LTU T4867AA Oracle v10g R2 EE Solaris 1-Sys LTU T4868AA Oracle v10g R2 EE Solaris 5-Sys LTU T4868AA Oracle v10g R2 EE Solaris 5-Sys LTU T4869AA Oracle v10g R2 EE Linux 1-Sys LTU

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 - October 2007

END AFFECTED VERSIONS

Note: Since Oracle for OpenView (OfO) is not installed using swinstall(1M) the HP-UX Software Assistant 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 - October 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 - October 2007."

For support contract information, please visit:
http://www.hp.com/managementsoftware/contract_maint

MANUAL ACTIONS : Yes - Update - Install the Oracle Critical Patch Update - October 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
Version:6 (rev.6) - 24 October 2007 "Critical Patch Update - October 2007" is available, added v10g and v10gR2

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.

HPSBMA02237 SSRT061260 rev.3 - HP OpenView Performance Agent (OVPA) Running Shared Trace Service, Remote Arbitrary Code Execution Remote arbitrary code execution

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.

->CVE-2007-3872

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, B.11.31), 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).

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

Note: The following is for use by the HP-UX Software Assistant. Only the HP-UX versions are listed.

AFFECTED VERSIONS

->HP-UX B.11.31
HP-UX B.11.23 (IA)
HP-UX B.11.23 (PA)
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

-> HP has provided a hotfix to resolve this vulnerability. Please contact the normal HP Services support channel and request the hotfix for "LCore SSRT061260 OpenView Shared Trace Service." The URL above is provided to expedite the service delivered by the HP support channel:

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
Version: 2 (rev.2) - 30 October 2007 Changed hotfix to "LCore SSRT061260 OpenView Shared Trace Service",changed revision to 03.10.040, added CVE-2007-3872
Version: 3 (rev.3) - 20 November 2007 Reformatted

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.

HPSBMA02236 SSRT061260 rev.2 - HP OpenView Performance Manager (OVPM) Running Shared Trace Service on HP-UX, Solaris, and Windows, Remote Arbitrary Code

Execution Document ID: emr_na-c01109171-2 Last Modified Date: Tue Oct 30 19:16:38 CET 2007 Submitted Date: Wed Jul 11 15:30:52 CEST 2007

SECURITY BULLETIN Remote arbitrary code execution

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.

-> CVE-2007-3872 HP OpenView Performance Manager (OVPM) 5.x and 6.x running on HP-UX PA-RISC and IPF (B.11.11,B.11.23, B.11.31), Solaris (5.7, 5.8, 5.9), Windows (2000, 2003 and Windows XP).

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

Note: The following is for use by the HP-UX Software Assistant. Only the HP-UX versions are listed.

AFFECTED VERSIONS HP-UX B.11.31 HP-UX B.11.23 (IA) 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:
http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

END AFFECTED VERSIONS

-> HP has provided a hotfix to resolve this vulnerability. Please contact the normal HP Services support channel and request the hotfix for "LCore SSRT061260 OpenView Shared Trace Service."

The following URL is provided to expedite the service delivered by the HP support channel:
http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

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
Version: 2 (rev.2) - 30 October 2007 Changed hotfix to "LCore SSRT061260 OpenView Shared Trace Service", added CVE-2007-3872

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: c01179918

Version: 1

HPSBMA02266 SSRT3646 rev.1 - Re-release of HPSBMI00005 OpenView Operations for Windows (OVOW), Remote Unauthorized Access

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

Release Date: 2003-10-08

Last Updated: 2007-10-02

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 OpenView Operations for Windows (OVOW). The vulnerability could be exploited remotely to gain unauthorized access.

References: HPSBMI00005

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. OpenView VantagePoint for Windows 6.1/6.2 OpenView Operations for Windows 7.0/7.1/7.2

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI0310-005 SSRT3646 rev.0.

The Hewlett-Packard Company thanks Mr. Rolf Langsdorf for reporting this vulnerability to security-alert@hp.com

OpenView Operations for Windows (OVOW) allows a local administrator of a managed node to execute an action on a remote managed node without having administrator rights on the remote node. A registry key allows this capability to be disabled. However, that feature does not work correctly.

Automatic or operator initiated actions can be triggered on an OVOW managed node for execution on a remote node also managed by OVOW. These remote actions can be triggered from all nodes to be executed on any other managed node. This might not be desired since not all local administrators of managed nodes may be trusted.

Also OVOW may be used to manage multiple management domains which must not have access to each other. There is a registry key which allows the disabling of automatic execution of remote actions in untrusted environments. However, this registry key does not function properly.

Also the registry key may not allow sufficient flexibility for many environments.

RESOLUTION

HP has made the following software updates available to resolve the vulnerability:

OpenView VantagePoint for Windows 6.1/6.2 English: VPW_00032 OpenView VantagePoint for Windows 6.1/6.2 Japanese: VPW_00033 OpenView Operations for Windows 7.0: OVOW_00062 OpenView Operations for Windows 7.1: OVOW_00050 OpenView Operations for Windows 7.2: OVOW_00064

These software updates are available on: http://itrc.hp.com/ and
http://support.openview.hp.com/patches/patch_index.jsp

Apply the applicable patch and disable remote actions in environments where either local administrators are not trusted or OpenView Operations for Windows is used to manage multiple management domains.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to MA.

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.

HPSBMA02238 SSRT061260 rev.3 - HP OpenView Reporter Running Shared Trace Service, Remote Arbitrary Code Execution Document ID: emr_na-c01109617-3

Last Modified Date: Tue Nov 20 21:16:49 CET 2007 Submitted Date: Wed Jul 11 18:17:31 CEST 2007

HPSBMA02238 SSRT061260 rev.3 - HP OpenView Reporter Running Shared Trace Service, Remote Arbitrary Code Execution Remote arbitrary code execution

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.

-> CVE-2007-3872

HP OpenView Reporter 3.7 running on Windows (2000, 2003, XP).

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.

-> HP has provided a hotfix to resolve this vulnerability. Please contact the normal HP Services support channel and request the hotfix for "LCore SSRT061260 OpenView Shared Trace Service."

The following URL is provided to expedite the service delivered by the HP support channel:

http://quixy.deu.hp.com/hotfix/d.php?P=lcore&N=SSRT061260+OpenView+Shared+Trace+Service&V=2.1

HISTORY

Version: 1 (rev.1) - 7 August 2007 Initial release
Version: 2 (rev.2) - 30 October 2007 Changed hotfix to "LCore SSRT061260 OpenView Shared Trace Service", added CVE-2007-3872
Version: 3 (rev.3) - 20 November 2007 Reformatted

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: c01205079

Version: 1

HPSBMA02279 SSRT071298 rev.1 - HP OpenView Configuration Management (CM) Infrastructure (Radia) and Client Configuration Manager (CCM) Running httpd.tkd, Remote Unauthorized Access to Data

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

Release Date: 2007-10-23

Last Updated: 2007-10-23

Potential Security Impact: Remote unauthorized access to data

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

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP OpenView Configuration Management (CM) Infrastructure (Radia) and Client Configuration Manager (CCM) running httpd.tkd. The vulnerability could be exploited to allow remote unauthorized access to data.

References: CVE-2007-5413

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP OpenView Configuration Management (CM) Infrastructure (Radia) v4.0, v4.1, v4.2, v4.2i running httpd.tkd on Windows, HP-UX, AIX, Solaris, and Linux. HP OpenView Client Configuration Manager (CCM) v2.0 running httpd.tkd on Windows.

BACKGROUND

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

The Hewlett-Packard Company thanks an anonymous researcher working with TippingPoint (www.tippingpoint.com) and the Zero Day Initiative (www.zerodayinitiative.com) for reporting this to security-alert@hp.com

Note: The httpd.tkd module is used by several OpenView Configuration Management (CM) and OpenView Client Configuration Management (CCM) Infrastructure components. These components include OS Manager, Policy Server, Portal, Patch Manager, Proxy Server, Distributed Configuration Server and Multicast Server. There may be more than one httpd.tkd module on a system. Each must be replaced. Please refer to the patch documentation for further information.

Note: The following is for use by the HP-UX Software Assistant. Only the HP-UX versions are listed

AFFECTED VERSIONS

For CM infrastructure (Radia) v4.0

HP-UX B.11.00
HP-UX B.11.11
HP-UX B.11.23
==========
action: install RADINFRAHPUX1_00009 or subsequent
URL: http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00009

For CM infrastructure (Radia) v4.1

HP-UX B.11.00
HP-UX B.11.11
HP-UX B.11.23

==========
action: install RADINFRAHPUX1_00010 or subsequent
URL: http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00010

For CM infrastructure (Radia) v4.2

HP-UX B.11.00
HP-UX B.11.11
HP-UX B.11.23
==========
action: install RADINFRASOL_00011 or subsequent
URL: http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRASOL_00011

End Affected Versions

RESOLUTION

HP has provided the following patches to resolve this vulnerability. The patches and installation instructions are available from the URL's listed below.

Product Platform Patch ID URL

CM Infrastructure v4.0 AIX RADINFRAAIX_00008 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAAIX_00008

CM Infrastructure v4.0 HP-UX B.11.00 RADINFRAHPUX1_00009 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00009

CM Infrastructure v4.0 HP-UX B.11.11 RADINFRAHPUX1_00009or or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00009

CM Infrastructure v4.0 HP-UX B.11.23 RADINFRAHPUX1_00009 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00009

CM Infrastructure v4.0 Linux RADINFRALNX_00007 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRALNX_00007

CM Infrastructure v4.0 Solaris RADINFRASOL_00009 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRASOL_00009

CM Infrastructure v4.0 Win32 RADINFRAWIN32_00023 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00023

CM Infrastructure v4.0i Win32 RADINFRAWIN32_00024 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00024

CM Infrastructure v4.1 AIX RADINFRAAIX_00009 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAAIX_00009

CM Infrastructure v4.1 HP-UX B.11.00 RADINFRAHPUX1_00010 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00010

CM Infrastructure v4.1 HP-UX B.11.11 RADINFRAHPUX1_00010 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00010

CM Infrastructure v4.1 HP-UX B.11.23 RADINFRAHPUX1_00010 or subsequent

http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00010

CM Infrastructure v4.1 Linux RADINFRALNX_00008 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRALNX_00008

CM Infrastructure v4.1 Solaris RADINFRASOL_00010 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRASOL_00010

CM Infrastructure v4.1 Win32 RADINFRAWIN32_00025 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00025

CM Infrastructure v4.2 AIX RADINFRAAIX_00010 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAAIX_00010

CM Infrastructure v4.2 HP-UX B.11.00 RADINFRAHPUX1_00011 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00011

CM Infrastructure v4.2 HP-UX B.11.11 RADINFRAHPUX1_00011 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00011

CM Infrastructure v4.2 HP-UX B.11.23 RADINFRAHPUX1_00011 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAHPUX1_00011

CM Infrastructure v4.2 Linux RADINFRALNX_00009 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRALNX_00009

CM Infrastructure v4.2 Solaris RADINFRASOL_00011 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRASOL_00011

CM Infrastructure v4.2 Win32 RADINFRAWIN32_00026 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00026

CM Infrastructure v4.2 with Patch 3.0.3 Win32 RADINFRAWIN32_00027 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00027

CM Infrastructure v4.2i Win32 RADINFRAWIN32_00028 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=RADINFRAWIN32_00028

CCM Infrastructure v2.0 Win32 CCM_00005 or subsequent
http://openview.hp.com/ecare/getsupportdoc?docid=CCM_00005

MANUAL ACTION: Yes – Update –

CM Infrastructure v4.0 HP-UX B.11.00 install RADINFRAHPUX1_00009 or subsequent
CM Infrastructure v4.0 HP-UX B.11.11 install RADINFRAHPUX1_00009 or subsequent
CM Infrastructure v4.0 HP-UX B.11.23 install RADINFRAHPUX1_00009 or subsequent
CM Infrastructure v4.1 HP-UX B.11.00 install RADINFRAHPUX1_00010 or subsequent
CM Infrastructure v4.1 HP-UX B.11.11 install RADINFRAHPUX1_00010 or subsequent
CM Infrastructure v4.1 HP-UX B.11.23 install RADINFRAHPUX1_00010 or subsequent
CM Infrastructure v4.2 HP-UX B.11.00 install RADINFRAHPUX1_00011 or subsequent
CM Infrastructure v4.2 HP-UX B.11.11 install RADINFRAHPUX1_00011 or subsequent
CM Infrastructure v4.2 HP-UX B.11.23 install RADINFRAHPUX1_00011 or subsequent

HISTORY

Version: 1 (rev.1) 23 October 2007 Initial release

Support: For further information, contact normal HP Services support channel.

HPSBMA02283 SSRT071319 rev.1 - HP OpenView Network Node Manager (OV NNM), Remote Cross Site Scripting (XSS) Remote cross site scripting (XSS)

A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM). This vulnerability could by exploited remotely to allow cross site scripting (XSS).

HP OpenView Network Node Manager (OV NNM) 6.41, 7.01, 7.51 running on HP-UX B.11.00, B.11.11, and B.11.23, Solaris, Windows NT, Windows 2000, Windows XP, and Linux.

Note: The following is for use by the HP-UX Software Assistant. Only the HP-UX versions are listed.

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 HP-UX OV NNM 7.51
HP-UX B.11.23 (IA)
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_36902 or subsequent

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_36901 or subsequent

For HP-UX OV NNM 7.01
HP-UX B.11.00
HP-UX B.11.11
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_36773 or subsequent

For HP-UX OV NNM 6.41
HP-UX B.11.00
HP-UX B.11.11
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_37141 or subsequent

END AFFECTED VERSIONS

HP has provided the following patches to resolve this vulnerability.

These patches are available from
http://support.openview.hp.com/patches/patch_index.jsp

OpenView Network Node Manager 7.51

HP-UX B.11.23 (IA) PHSS_36902 or subsequent
HP-UX B.11.23 (PA) PHSS_36901 or subsequent
HP-UX B.11.11 PHSS_36901 or subsequent
HP-UX B.11.00 PHSS_36901 or subsequent
Linux RedHatAS2.1 LXOV_00054 or subsequent
Solaris PSOV_03482 or subsequent
Windows NNM_01161 or subsequent

OpenView Network Node Manager 7.01

HP-UX B.11.11 PHSS_36773 or subsequent
HP-UX B.11.00 PHSS_36773 or subsequent
Solaris PSOV_03480 or subsequent
Windows NNM_01159 or subsequent

OpenView Network Node Manager 6.41

HP-UX B.11.11 PHSS_37141 or subsequent
HP-UX B.11.00 PHSS_37141 or subsequent
Solaris PSOV_03489 or subsequent
Windows NNM_01167 or subsequent

MANUAL ACTIONS: Non-HP-UX only - Install the patches listed in the Resolution section for Solaris, Windows, and Linux.

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) - 28 November 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

HP Security Bulletins – JetDirect

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179557

Version: 1

HPSBPI02263 SSRT3512 rev.1 - Re-release of HPSBMI0002 HP Jetdirect, Remote Unauthorized Access, Denial of Service (DoS)

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

Release Date: 2003-03-11

Last Updated: 2007-10-02

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 Jetdirect. The vulnerability could be exploited to allow remote unauthorized access or to create a Denial of Service (DoS).

References: HPSBMI00002

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP Jetdirect 310x Print Server for Fast Ethernet (J6038A) with Q.24.06 firmware.

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI0303-002 SSRT3512 rev.0.

RESOLUTION

To resolve the vulnerability update to Q.24.09 firmware or subsequent.

Please refer to the following for more information:

Upgrading Jetdirect Firmware

1. Via the HP Download Manager
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06917

2. Via Web Jetadmin
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06529

Making Jetdirect Print Servers Secure on the Network
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999

Using the HP Jetdirect Embedded Web Server Security Wizard
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07576

MANUAL ACTIONS: Yes – Update - Update to Q.24.09 firmware or subsequent.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with SPC change from MI to PI.

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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179857

Version: 1

HPSBPI02265 SSRT3515 rev.1 - Re-release of HPSBMI00004 HP Jetdirect Running ftp, Advisory

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

Release Date: 2003-04-22

Last Updated: 2007-10-02

Potential Security Impact: Advisory

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

VULNERABILITY SUMMARY

Some security scanners generate warnings that the Jetdirect ftp directory is writable.

References: HPSBMI00004

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP Jetdirect running ftp.

BACKGROUND

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

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI0304-004 SSRT3515 rev.0.

Any file sent to the Jetdirect ftp service is printed. Because certain ftp directories have write permissions some security scanners report errors.

RESOLUTION

To restrict printing or suppress the security scanners warning, the ftp service can be disabled.

To disable ftp, telnet to the Jetdirect device and type:

ftp-config: 0

When this change is made printing via ftp will no longer function. It will also not be possible to update firmware via ftp. The firmware can be updated using the HP Download Manager or Web Jetadmin.

Please refer to the following for more information:

HP Jetdirect Print Servers - Security Technical Brief
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00004828

Upgrading Jetdirect Firmware

1. Via the HP Download Manager
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06917

2. Via Web Jetadmin
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj06529

Making Jetdirect Print Servers Secure on the Network
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999

Using the HP Jetdirect Embedded Web Server Security Wizard
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07576

MANUAL ACTIONS: Yes – NonUpdate - Disable the ftp service if desired.

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to PI.

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 Instant Toptools, Local denial of service

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01179796

Version: 1

HPSBGN02264 SSRT3493 rev.1 - Re-release of HPSBMI00003 HP Instant Toptools, Local denial of service

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

Release Date: 2003-03-31

Last Updated: 2007-10-02

Potential Security Impact: Local denial of service

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

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP Instant Toptools. The vulnerability could be exploited locally to create a denial of service (DoS).

References: HPSBMI00003

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. Windows Server 2003, Windows 2000, Windows NT4 running HP Instant Toptools.

BACKGROUND

For a PGP signed version of this security bulletin please write to:

security-alert@hp.com

Note: This Security Bulletin has been re-released with a new document number but without alteration of content. The purpose of this new number and re-release is to assure the document is available on all customer accessible databases.
This is a reformatted version of Security Bulletin HPSBMI0303-003 SSRT3493 rev.1.

The Hewlett-Packard Company thanks Erik Parker of Digital Defense, Inc. for reporting this vulnerability to security-alert@hp.com

RESOLUTION

HP has made the following software updates available to resolve the vulnerability.

The software updates are available on:

http://h20004.www2.hp.com/soar_rnotes/bsdmatrix/

Windows Server 2003, Windows 2000, Windows NT4 HP Instant Toptools version 5.55 or subsequent

HISTORY

Version: 1 (rev.1) - 02 October 2007 Initial release, with an SPC change from MI to GN.

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.