EPING May 2007

This is an archived edition of EPing, first published in May 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 – Linux – An idea whose time has come?

Has Linux now reached the mainstream? I could probably have written these comments at any time during the last five years, indeed I probably have in previous columns. But earlier articles would have been tempered by the recognition that, although everyone was saying Linux had 'arrived', our experience through hpUG events was telling a very different story. Attendance at hpUG Linux events was poor, but this no longer seems to be the case. Within the last six months we have run two Linux events which have been very well attended. Perhaps this marks a change from Linux being considered only for 'new' applications to a time when those of us who run HP-UX or OpenVMS systems are now looking at it seriously as a viable alternative. Whatever the reason, hpUG will be running more Linux events and providing more information through E-PING.

It sounded like an Oscar speech, but there were a lot of people I had to thank. The User Group AGM took place on 24 April at HP Bristol Labs and as a result of nominations I am very pleased to welcome Jane Ayres of OCSL to the Management Group. But sadly it was also time to say goodbye to two valued members. John Ferguson, after many years of service to the DECUS and the HP User Groups has decided to stand down from the Management Group and has also relinquished the post of Company Secretary. Rob Atkinson too has left the Management Group. Rob joined us just 3 years ago and in the last year has made a significant contribution as the architect of our new web site and of E-PING. We will miss them both, and I wish them well.

I look forward to hearing from you.

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

Total Cost of Ownership White Paper

with thanks to Susan Skonetski

There is a new white paper from TechWise Research on "Quantifying the Total Cost of Upgrading HP OpenVMS Alpha Server Systems to OpenVMS on HP Integrity Servers".

If you have ever heard me do a directions session, one of the things that I recommend is that you print off the Total Cost of Ownership white papers and give them to your managers. This is one of those white papers and I highly recommend that you read it and pass it on - it is very valuable.

It is available on the HP OpenVMS web site at:

http://h71028.www7.hp.com/ERC/downloads/OpenVMS_TCU_2007.pdf

OpenVMS Performance Enhancement Service

This worldwide service from Bruden-OSSG is called PRONE - Performance Results Or No Expense.

Bruden offer to visit the customer site, look at the application and attempt to improve performance. If performance isn't improved by at least 10%, then the service is free.

A specific example was as follows: The customer was running on Alpha with an application that does not scale above more than 1 CPU. Bruden ported the customer to Itanium (not related to the performance problem), implemented the service and was able to make the application scale. The application received a total of 460% increase in performance compared to the Alpha and 260% increase just on Itanium.

HP OpenVMS Integrity

Useful Information - OpenVMS on Integrity Servers – with thanks to Sue Skonetski

Please note the "with thanks from openvms.org" - you will see several new ports to OpenVMS on IPF.

With thanks to the HP OpenVMS Web site, obviously this is not the full extent of available information but I thought it was very interesting.

- If you only click on one link make it this one:

http://h71000.www7.hp.com/announce/cust_statements.html

- OpenVMS on Blade Systems:

http://h71000.www7.hp.com/openvms/cclass_support.html

- OpenVMS on Superdomes:

http://h20341.www2.hp.com/integrity/cache/342254-0-0-225-121.html

- HP Servers running OpenVMS:

http://h18000.www1.hp.com/products/servers/byos/openvmsservers.html

- 16 page white paper about VMS and Virtualization:

http://h71028.www7.hp.com/ERC/downloads/4AA0-5801ENW.pdf

- If you are looking for a Partner to see if it is porting to Integrity check out this page:

http://h71000.www7.hp.com/solutions/matrix/i64partner_a.html

There is an A-Z list (it's only small). If you are a partner and your status is incorrect please let me know, it can be fixed.

- Erratas:

http://h71000.www7.hp.com/doc/hardware.html

With thanks to www.openvms.org

- Ported to OpenVMS on IPF:

The Distributed Revision Control Management System, Mercurial, has been ported on OpenVMS IA64 (and AXP). Mercurial is a fast, lightweight Source Control Management system designed for efficient handling of very large distributed projects.

For more information on Mercurial please see www.selenic.com/mercurial

- MoinMoin Wiki Engine has been ported to OpenVMS, AXP and IA64.

For more information on MoinMoin please see moinmoin.wikiwikiweb.de

- The vmspython site has been changed to use MoinMoin.

For more information on MoinMoin on OpenVMS please see vmspython.dyndns.org

- Webware for Python 0.9.3 is released on OpenVMS, AXP and IA64.

www.w4py.org

HP OpenVMS Integrity and Synergy - Hudson Printing

with thanks to Susan Skonetski

The following is from the Synergy Newsletter and Web site:

http://www.synergex.com/Company/Articledetail.asp?id=2828

Customer Success Story - Hudson Printing migrates their Synergy applications to OpenVMS on the Integrity server

Hudson Printing, founded over 100 years ago in Salt Lake City, UT, is a commercial Web-press operation which prints many short to medium run publications and recently completed the migration of some of their Synergy/DE-based applications from HP OpenVMS Alpha to HP OpenVMS on the Integrity server. Migration of the other applications will soon follow.

Hudson Printing uses Synergy/DE-based applications from Pelikan Technology to run all of their in-house systems, including handling job quotes; tracking individual jobs; managing time and attendance records; tracking inventory of raw paper, finished goods, and processed goods; and managing shipping and accounting systems.

Hudson's applications were previously running on two OpenVMS Alpha servers, which were over 12 years old. Wanting to update the systems while continuing to harness the flexibility and stability of the OpenVMS platform, Hudson chose to migrate to Integrity. "Our customer likes the VMS platform

because it is so reliable," states Pelikan Technology president Joe West. "They work 24/7 and the Synergy/DE-based applications we developed run both the front office and the production areas-having the system up all of the time is very important."

The migration is being done in phases, as Pelikan is continuing to make adjustments to some of Hudson's applications before porting to the new platform. "So far everything has gone smoothly," states West. "The Integrity is performing very well."

West concludes: "Offering our customers this migration path to the Integrity enables them to extend their OpenVMS investment and capitalize on the performance and cost benefits of the server. Together, Synergy/DE and OpenVMS enable us to keep our applications up to date and competitive."

HP Customer Case Study - Leading Austrian logistics expert easily transitions from AlphaServer to HP Integrity servers.

“The transition from AlphaServer to our new Itanium-powered HP Integrity servers was very straightforward. The OpenVMS operating system is extremely stable. We now expect to reap the rewards of the new configuration Integrity servers will bring us.” Robert Zöbinger, software developer, Knapp Logistik Automations GmbH

Industry

MDI: Logistics Knapp Logistik Automations has over fifty years of experience in delivering warehouse logistics and automation solutions. With a broad portfolio of services, including warehouse layout design and installation, staff training, software and technical operations, it has earned a reputation for delivering both innovation and efficiency to a wide range of global clients.

Solving future problems now

Knapp Logistik was facing significant IT issues that would, if not resolved, impact IT and business performance. The mission-critical application used and trusted to control the company’s internal order processing, production planning, warehouse maintenance and stock replenishment was written in DEC COBOL – an aging computer language that severely limited the application’s interoperability with other programming languages and databases, and also inhibited its portability to new or different platforms. The application’s inherent lack of flexibility and restricted capacity for expansion needed to be addressed. In addition, the HP AlphaServer platform comprising two HP AlphaServer DS20, was being retired and so a transition to a newer, fully supported platform was also necessary.

A future-proof investment

To resolve these issues and make the necessary improvements, Knapp Logistik sought the trusted expertise of Acucorp, a strategic partner of HP, and a leading provider of COBOL modernisation solutions. Together, the two parties updated and upgraded the existing COBOL application – Acucorp extend® toolset, and deployed thin client technology incorporating a new Windows-style Graphical User Interface (GUI) to replace Knapp’s old characterbased screens. Robert Zöbinger, software developer, Knapp Logistik Automations, says, “Updating our COBOL application avoided a costly re-write and also future-proofed our investment by adding the capability for interoperability and portability. This ensured that we could easily transition to a new platform when we were ready.”

Approach

Employed HP strategic partner Acucorp to modernise the COBOL application and develop and deploy thin client technology incorporating a Windows-style Graphical User Interface.

Selected two HP Integrity servers powered by Dual-Core Intel®Itanium® 2 processors running on OpenVMS to replace the AlphaServer environment.

Selected an HP StorageWorks EVA8000 storage array to provide enhanced capacity for data storage.

To learn more, visit www.hp.com

as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Publication Number: 4AA1-0946ENW Written: April 2007

PRAISE FOR USER GROUP EVENT MANAGEMENT

hpUG event in Bristol – 11 January 2007

Eva Beck wrote to the User Group to thank us for all the hard work that went into the OpenSource Roadshow in Bristol in January.

She said – "*… given the number of attendees and the customers you got (about 150 attendees, including speakers) this was an extremely successful event! I talked to some of the customers who were very positive about the setup - seems it was also appreciated that this was not a "sales event" but an event to educate technically interested people. Working with the hpUG team to set up events seems to be an interesting format to address new people. Thanks for your efforts. This was an absolutely successful event…*"

Eva Beck is Business Manager Open Source and Linux ESS Europe, Middle East, Africa, Hewlett-Packard EMEA GmbH, Dornach

Yahoo – More Than Just a Search Engine?

What seems like a long time ago now, Yahoo fought it out with some of the other young 'uns in the Internet Search Engine war. The likes of AltaVista and AOL laid bleeding at the side of the road, whilst Yahoo took control of the market. To its dismay, along came Google with its bright, shiny and simplistic approach to doing things - and Web War II began.

Google quickly realised that just providing the tools for searching for information was not good enough, and embarked on developing its own unique content. From this the likes of Google Earth and Google Sketchup were born.

Now it's Yahoo's turn to throw a few punches, and it's established the Yahoo Developer Network (YDN) to take on the task.

According to Yahoo, "The Yahoo! Developer Network offers Web Services and APIs that make it easy for developers to build applications and mashups that integrate data sources in new ways, making the web a more useful and fun place for everyone."

As you can see, rather than reinvent the wheel, I've let Yahoo give you the low-down, and this is exactly what the Developer Network is all about. A growing number of computer users are now able to create their own space on the Internet, whether through point-and-click interfaces or by programming the content from the comfort of their armchairs. However, none of us like to write from scratch when there's already something available for us to use, and Yahoo has latched onto that fact.

Yahoo doesn't limit itself to one set of standards, as with the Microsoft Developer Network, but allows you to get involved in all of the popular languages like .Net, Python, PHP, etc.

One part of the Developer Centre is the **Yahoo User Interface Library**. This is a collection of professional utilities that allow you to easily turn your web pages from flat, uninteresting content into

interactive, eye catching media. You can integrate ***Drag-and-Drop*** elements that allow you to build a snazzy shopping cart, create ***Tabbed Content*** that allows your users to view multiple types of content without having to reload the page into the browser, and even AJAX calls using the ***Connection Manager*** API. All of the components are fully documented; so as long as you understand the terminology, you shouldn't have too much trouble integrating it with your pages.

One of the areas that makes the YDN stand out is the YUI Theatre, a collection of video training sessions on technology subjects. The information in Doug Crockford's *The JavaScript Programming Language* video is extremely enlightening, even for the most hardened web developer. Rather than trying to create a 'show', as some other sites of a similar ilk have previously done, you get the information in a fast and to the point package, exactly as you would if you were in a classroom situation.

OK, so most of this isn't exactly new, but the way Yahoo have put the whole package together gives them an edge on some of the other big players in the field. It's time to sit back and see what Google respond with, but if the current trend continues, it can only be good news for the users of these systems.

Written By
Robert Atkinson

Emulex Offerings at HP Technology at Work event in Berlin

EMULEX were showing:

HBA management suite HBAnyware, recognized as the industries leading product:

- Simple Batch mode, for updating multiple HBA's parameters at a single key stroke.
- In and out of band auto discovery
- Non disruptive f/w and bios loads without the need to reboot

Please see report from an independent consultancy firm that compared this to other products in the market: http://www.emulex.com/white/hba/HBAnywareSoftEval.pdf

They were also demonstrating, their tight integration into virtualization environments. Please use the following link to see the impact of virtualization on I/O performance: http://www.emulex.com/white/hba/vmware_performance.pdf

Further information is available at: http://www.emulex.com/

Hints and Tips – Security

HP-UX ServiceGuard - Design Considerations with NIS

PROBLEM
I am trying to share password and group information within my ServiceGuard cluster on HP-UX v 11.11 or v 11.23. What things should be considered in using NIS or NIS+ to do this?

SOLUTION
Here are some notes on how you can use Network Information Service (NIS) within your HP-UX v 11.11 or v 11.23 ServiceGuard Cluster, with a few conditions.

General restrictions on using NIS not limited to ServiceGuard:

NIS is not supported with HP-UX Trusted System. If when examining the /etc/passwd file find that ALL the passwords have been replaced by "*", then this indicates the system is trusted.

NIS is not supported if the ShadowPassword bundle has been implemented on HP-UX v 11.11 or v 11.23. If you examine the /etc/passwd file and find that ALL the passwords have been replaced by "+", then you have enabled Shadow Password. Note however, that NIS support for ShadowPassword is available with HP-UX v 11.31.

If you decide to use NIS, review the roles of the NIS client, the NIS Server, and of the NIS Master server, and the potential for single point of failure with the NIS Master Server.

Click here for more information on the roles of NIS client, Slave and Master Servers found in chapter 4 "Configuring and Administering NIS" in the "NFS Services Administrators Guide" manual at http://docs.hp.com/ .Look for the Manual on the main page.

Design considerations for NIS Server placement when using ServiceGuard:

The NIS Master server is a single point of failure since no password, nor other NIS database changes can be made if it is offline or unavailable. All database changes with NIS are made on the Master Server only, and propagated, or "pushed", to the Slave NIS Server(s), if any. Password changes are implemented by interaction between the passwd or yppasswd command on the NIS client and the rpc.yppasswdd daemon running on the NIS Master. If the NIS Master service is not available, these changes cannot be made.

The NIS database design does not lend itself well to implementing NIS Master and Slave servers within packages in a cluster. This is because the NIS database internally caches the hostname of the NIS Master in the database and also creates a ypservers map containing the names of the NIS Master and of all NIS Slave servers. This is not configurable.

Hosts in the cluster may be NIS slave servers in order to provide redundancy for NIS database lookups should the NIS Master be unavailable.

NIS Master server should also have be accessible on the private heartbeat LAN(s), if any are present. This is because Sun RPC assumes all networks are routable.

Click here to see the Chapter 4 of the "Managing ServiceGuard" manual at: http://docs.hp.com/en/ha.html#ServiceGuard for an explanation.

NIS Client considerations:

All clients should use ypinit -c to create the list of NIS Servers to bind to, in

preferential order. These hostnames MUST be in /etc/hosts, and include all active networks including Heartbeat networks. Unless the NIS Server is running as part of a ServiceGuard package (not recommended) you shouldn't need to specify any package IP hostnames. This step must be followed on all NIS clients, including those systems that are also acting as NIS servers.

For 11.11 nodes, you will most likely need to update the ypinit script since the ypinit -c functionality was released in a patch, and placed into /usr/newconfig/usr/sbin/ypinit. Save your /usr/sbin/ypinit script, and take note of any customizations you might have made to it, such as adding any new maps. Copy the ypinit script over from /usr/newconfig/usr/sbin into /usr/sbin and merge in those customizations, if any.

Systems acting as NIS slaves or as the NIS Master, should first try to bind to themselves. Systems in the cluster NOT acting as NIS Servers, should bind to any NIS Server systems in the cluster, if any.

All clients, and NIS Servers should generally use the /etc/nsswitch.files template for /etc/nsswitch.conf, with these considerations:

For password and group when using the "+" "-" entries to include or exclude users and netgroups, you should use:

```
passwd:   compat
group:    compat
netgroup: files nis
```

If not using the "+" "-" syntax in your /etc/passwd then you should use:

```
passwd:   files nis
group:    files nis
netgroup: files nis
```

Include "nis" for any other databases that are actually using NIS. Sometimes services are also managed by NIS, so you may want to add:

```
services:  files nis
```

Remember to use the "hosts" entry that is appropriate for your installation! We recommend looking at "files" first, before NIS or DNS. For example:

```
hosts:    files nis dns
```

What about using NIS+ or LDAP to share password or group databases?

The answer is that you could use either NIS, NIS+, or LDAP-UX. However, HP does not recommend the use of NIS+ for several reasons, the most important of which is that it has been discontinued in the present OS release (11.31) and LDAP has replaced it.

Implementing ldap-ux is the suggested migration path.

HP-UX: support for shadow passwords with NIS

PROBLEM
With respect to Shadow Passwords with NIS in a heterogeneous NIS environment including:

HP-UX 11.11 NIS Master server
Sun NIS Slave server
NIS clients

the following document:

HP-UX Software Transition Kit > HP-UX 11i v1.6 critical impact

http://devrsrc1.external.hp.com/STK/impacts/i833.html

states that at some point, support for shadow passwords with NIS will be available.

When will this occur and with which release?

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - NIS (Network Information Service)

RESOLUTION
Here are a few observations regarding HP's NIS implementation:

1. NIS is basically not secure with regards to the current security needs.

2. Shadow Password for NIS is NOT supported on the current HP-UX versions - 11.0, 11.11 (also known as 11i version 1), 11.23 (11i version 2). The software changes necessary to provide Shadow Password support with NIS on the current HP-UX versions would be considerable, and, at the time of this writing, it has been decided not to change the current versions. Currently, plans are in place to provide Shadow Password for NIS with the next HP-UX version, that is, HP-UX 11.31, also known as 11i version 3.

3. Some interoperability issues would remain in hybrid NIS environments such as NIS environments with other vendors' systems.

4. HP's direction, as well as their competitors', is to move from NIS to LDAP.

5. Regarding NIS+: NIS+ (NIS Plus) addressed some security issues, but NIS+ has been discontinued by HP. Other vendors recommend moving from NIS+ to LDAP.

At the time of this writing, plans are in place to provide Shadow password support for NIS in HP-UX version 11.31 to come, but LDAP-UX will remain HP's recommended, long-term solution.

NOTE: HP provides NO guarantees of any kind regarding future support for Shadow passwords.

HP's recommended solution is to move from NIS to LDAP-UX. The main reason is that LDAP is a more complete, secure, and standard solution, recommended by HP as well as by other major vendors.

LDAP-UX is the LDAP solution on HP-UX systems. The HP LDAP-UX Integration bundle contains tools to migrate from NIS to LDAP as well as the NIS/LDAP Gateway product. For more information, please refer to the HP Software Depot at:

http://software.hp.com/

Search for "LDAP-UX Integration" and obtain the following documents:

HP-UX Shadow Passwords
LDAP-UX Integration for HP-UX

Also refer to:

NIS/LDAP Gateway Administrator's Guide

available at:

http://docs.hp.com/en/J4269-90028/index.html

HP-UX NIS Client - Sun NIS Server with C2 Security: interoperability issues

PROBLEM
Here are three questions related to interoperability issues with respect to the following example configuration:

A. NIS Server: Sun Solaris 9 + C2 secure activated (passwd.adjunct feature)

B. NIS Clients: HP-UX 11.11 systems

1. one r-commands client - remsh command

2. one r-commands server - remshd daemon

The questions are:

Q1. Can an HP-UX system be used as an NIS Client of a Sun Solaris NIS Server that satisfies the Class C2 security criteria?

Q2. What alternate solution can be advised?

Q3. Why not use NISplus (NIS+) instead?

CONFIGURATION
Operating System - HP-UX
Version - 11.11
Subsystem - NIS

RESOLUTION
Please see the answers provided below each question:

Q1. Can an HP-UX system be used as an NIS Client of a Sun Solaris NIS Server that satisfies the Class C2 security criteria?

A1. There are several ways to implement C2 security. The Sun-specific C2 implementation, that comprises the passwd.adjunct feature, is not supported on any HP-UX version. At least one issue described in the following document may be encountered:

Doc_id: 4000097215A
Title: remsh returns "Account is disabled"
available at: http://www.itrc.hp.com/

Q2. What alternate solution can be advised?

A2. The main solution is to migrate from NIS to LDAP. The LDAP solution on HP-UX is called LDAP-UX.

The HP LDAP-UX Integration bundle contains tools to migrate from NIS to LDAP as well as the NIS/LDAP Gateway product. For more information, please go the HP Software Depot at:

http://software.hp.com/

and search for "LDAP-UX Integration".

Q3. Why not use NISplus (NIS+) instead?

A3. The NISPlus product has been discontinued. NIS+ is replaced by LDAP-UX as well.

Here are the main reasons about why HP does not recommend to install and use NIS+ :

A few years ago, the Sun NIS+ (NIS Plus) product was intended to provide a more secured, enhanced NIS-like product. However, it appears that NIS+ is no longer promoted; similarly, HP no longer provides NIS+ in HP-UX.

LDAP is an excellent replacement for NIS along with security features, but it implies the use of centralized user repositories. Since most Unix market leaders, such as Sun, IBM, and HP, advise customers to migrate to LDAP, there is no plan to make HP-UX compliant with Sun's C2 implementation. This means that, at the time of this

writing, HP has no current plans to add support for the "passwd.adjunct" map because the industry is migrating from NIS to LDAP.

For NISplus / NIS+, please also refer to the LDAP-UX integration product.

The "NIS+ to LDAP Migration Guide" - available at http://docs.hp.com/ - describes the migration procedures used to migrate the NIS+ server to the LDAP directory server and to install LDAP-UX Client Services on HP-UX NIS+ clients.

HP-UX - Automount - 'couldn't bind to reserved port' and 'rpcbind: t_bind t_errno = 23'

PROBLEM
The following behavior occurs on HP-UX Superdome systems with Enhanced AutoFS, such as AutoFS 2.3 for HP-UX 11.11, and NIS clients (NIS ONC 1.2) on HP-UX 11.11 or 11.23 systems. On a Superdome (SD) partition that intensively operates with AutoFS automounts and with Name Resolution via NIS, the mount operations sometimes fail and log at least one of the following error messages:

o in syslog.log:

"automountd ... : mount ...: Couldn't bind to reserved port"

"rpcbind: check_bound: t_bind: exit, t_errno = 23"

o in automount.log:

"getmount_alloc() failure"

CONFIGURATION
Operating System - HP-UX 11.11
Application - Enhanced AutoFS

RESOLUTION
There is a very intensive use of the UDP reserved ports done by NIS (NIS Client) for name resolution, as well as by the AutoFS automounter. As a consequence, sometimes there are not enough UDP reserved ports left to service all the automount requests, thus the user may see the message:

cannot mount /home/<user> directory

In the "rpcbind: check_bound: t_bind: exit, t_errno = 23" error message, "t_errno = 23" is an XTI/TLI error indicator which means that the address is already in use. The transport provider cannot bind the specified address, hence the provider reports that the address is busy.

The root cause of this behavior is that when using NIS for name resolution, the system may run out of udp ports. This is a scalability issue with NIS ONC 1.2 product limitation. Reserved ports are kept open until the calling process exits.

Here are two solutions:

1. Use DNS prior to NIS, i.e. change the /etc/nsswitch.conf file. Be aware that it is VERY IMPORTANT to keep the DNS configuration as reliable and up to date as possible. In many environments, this task is more difficult that with NIS.

2. Perform an NIS to LDAP-UX migration.

HP-UX passwd command errors when nsswitch.conf contains winbind as a backend store

PROBLEM
On HP-UX 11.11, if the file /etc/nsswitch.conf contains a winbind entry in the passwd line, the HP-UX passwd(1) command may not work, and instead report an error message similar to the following:

```
# passwd
Supported configurations for passwd management are as follows:
passwd: files
passwd: files ldap
passwd: files nis
passwd: files nisplus
passwd: compat
passwd: compat AND
passwd_compat: nisplus
```

This behavior can occur when attempting to change root's passwd or when entering a normal user password.

CONFIGURATION
Operating System - HP-UX
Version - 11.11
Application - CIFS Server A.02.xx

RESOLUTION
The behavior described above occurred because libpam_unix was checking for specific "registered" configurations for backends in nsswitch.conf; since winbind was not listed as one of these configurations, the passwd command, which goes through libpam_unix, would fail with the above error. This behavior was in fact also an issue for OTHER backend configurations such as that described in the SR referenced below.

The behavior described above is resolved by applying the following libpam vi patch:

[PHCO_33215/PACHRDME/English]
s700_800 11.11 libpam_unix cumulative patch

along with its dependency:

[PHNE_33971/PACHRDME/English]
s700_800 11.11 ONC/NFS General Release/Performance Patch

which contains a fix for the following SR (Service Request):

Doc_id: [8606227681/STARS/English] (CR# JAGad96745)
Title: passwd command produces error when nsswitch.conf has files nis ldap

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

Note:
Apply these patches and any required dependencies. These patches, as with any patch, may be superseded. Please check for the latest patches at HP's IT Resource Center (ITRC) at the following web site:

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

Unix passwd may give errors when using winbind in nsswitch.conf

PROBLEM
On HP-UX 11.11, if the file /etc/nsswitch.conf contains a winbind entry in passwd line, the HP-UX command "passwd" may not work, and instead report an error message, whether you are changing root or a normal user password:

```
# passwd
Supported configurations for passwd management are as follows:
   passwd: files
   passwd: files ldap
   passwd: files nis
   passwd: files nisplus
   passwd: compat
   passwd: compat AND
   passwd_compat: nisplus
```

CONFIGURATION
CIFS Server A.02.XX running Winbind

RESOLUTION
The solution is to apply [PHCO_33215/PACHRDME/English] and it's dependency [PHNE_23502/PACHRDME/English], which contains a fix for the following JAG: JAGad96745.

Apparently when they 'relaxed' the nsswitch.conf checking by libpam_unix.1 to fix this problem, it also allowed libpam_unix to work with winbind.

Root Cause: libpam_unix was checking for specific 'registered' configurations for backends in nsswitch.conf; since winbind was not listed as one of these

configurations, the passwd command, which goes through libpam_unix, would fail with the above error. This behavior was in fact also a problem for OTHER backend configurations, such as that described in JAGad96745. Fixing this behavior in libpam_unix vi patch [PHCO_33215/PACHRDME/English] resolves this issue.

How to configure PAM passwdqc password strength checking

PROBLEM
For security reasons I wish to enforce strong passwords. HP-UX trusted system does not offer all the password checks I am looking for.

I found the PAM_passwdqc product on the HP-UX 11i v1 and 11i v2 Internet Express offering:

HP-UX Internet Express A.06.00 Product Overview

PAM_passwdqc

PAM_passwdqc is a password strength checking module for PAM-aware password changing programs, such as passwd(1). PAM_passwdqc checks regular passwords, offers support for passphrases, and can provide randomly generated passwords.

It covers my requirements but is an open source product. I read the documentation but am still unsure how to add passwdqc to existing PAM modules on HP-UX 11.11 and 11.23.

RESOLUTION

As an Open Source security component the PAM passwdqc module is not covered under HP-UX support contracts. For documentation see:

passwdqc README

Below is an example of how passwdqc can be added to the existing PAM configuration file. Testing has been limited and the information is provided as is.

Install passwdqc

Download ixPAMpasswd from the software depot or install it from the Internet Express CD:

swinstall -s /tmp/ixPAMpasswd_A.06.00-1.0.2.001_HP-UX_B.11.23_IA+PA.depot * Verify the library

ls /usr/lib/security/hpux64/pam_passwdqc.so.1
ls /usr/lib/security/hpux32/pam_passwdqc.so.1

Check the README

The README can be found in /opt/iexpress/pampasswd. Decide which options to use in your environment.

The openwall site states:

> On HP-UX 11, pam_passwdqc has to ask for the old password during the update phase. Use "ask_oldauthtok=update check_oldauthtok" with pam_passwdqc and "use_first_pass" with pam_unix.

Modify /etc/pam.conf

The README states:

> This module should be stacked before your usual password changing module (such as pam_unix or pam_pwdb) in the password management group (the "password" lines in /etc/pam.d/passwd or /etc/pam.conf).

This is an example of an HP-UX 11.23 system /etc/pam.conf including passwdqc.

```
# more /etc/pam.conf

#
# Password management
#
login    password required   pam_passwdqc.so.1 ask_oldauthtok=update
check_oldauthtok min=disabled,disabled,disabled,6,6 max=8 passphrase=0
similar=permit enforce=users
login    password required   libpam_hpsec.so.1
login    password required   libpam_unix.so.1 use_first_pass
passwd   password required   pam_passwdqc.so.1 ask_oldauthtok=update
check_oldauthtok min=disabled,disabled,disabled,6,6 max=8 passphrase=0
similar=permit enforce=users
passwd   password required   libpam_hpsec.so.1
passwd   password required   libpam_unix.so.1 use_first_pass
dtlogin  password required   libpam_hpsec.so.1
dtlogin  password required   libpam_unix.so.1
sshd     password required   pam_passwdqc.so.1 ask_oldauthtok=update
check_oldauthtok min=disabled,disabled,disabled,6,6 max=8 passphrase=0
similar=permit enforce=users
sshd     password required   libpam_hpsec.so.1
sshd     password required   libpam_unix.so.1 use_first_pass
OTHER    password required   libpam_unix.so.1
```

Note: The options after pam_passwdqc.so.1 are all on one single line.

Choose each service you wish to enable strong password checks for. The passwd service covers the passwd command. Adding the module to login and sshd causes them to check for passwords using passwdqc instead of the regular HP-UX checks when a user's password has expired and needs to be changed during login.

Use use_first_pass option for pam_unix:

use_first_pass
It compares the password in the password database with the user's initial password (entered when the user authenticated to the first authentication module in the stack). If the passwords do not match, or if no password has been entered, quit and do not prompt the user for a password.

The option does not apply to pam_hpsec.

The file would look very similar on HP-UX 11.11. The difference is that HP-UX 11.11 does not have a pam_hpsec. Some systems may not have sshd in the pam configuration either.

For further information regarding PAM, check the manual pages:
pam(3)
pam.conf(4)
pam_user.conf(4)
pam_unix(5)
pam_hpsec(5)

Test the PAM passwdqc module

passwd user1

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a 6 character long password with characters from at least 3 of these 4 classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password:
Re-type new password:
Changing password for user1
Passwd successfully changed

If a user's password has expired, login or ssh will prompt:

login: user1
Password:
Your password has expired. Choose a new one
Enter current password:

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a 6 character long password with characters from at least 3 of these 4 classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password:

Back out PAM changes

If for any reason the passwdqc module has to be removed, copy your current /etc/pam.conf to another location and restore the original from:
/usr/newconfig/etc/pam.conf
The effect on passwd, login etc is instant.

Disclaimer: While the above configuration has been tested with various scenarios, no extensive testing has been performed. Neither the passwdqc module nor the changes to pam.conf are supported by HP. HP does support questions regarding the PAM framework.

Note: Some of this functionality is already available in the 11.23 HP supported PAM module pam_hpsec. The following options (defined in the security (4) manual page) can be used to configure password restrictions:

MIN_PASSWORD_LENGTH
PASSWORD_MIN_UPPER_CASE_CHARS
PASSWORD_MIN_LOWER_CASE_CHARS
PASSWORD_MIN_DIGIT_CHARS
PASSWORD_MIN_SPECIAL_CHARS

These values need to be configured in the file /etc/default/security. The default value for MIN_PASSWORD_LENGTH is 6 characters (does not apply to trusted systems) and the default for the other values is 0.

Additional security can be provided by installing the the HP Standard Mode Security Extensions software. This software is downloadable from HP's software depot (and is included in the May 2005 OE and later):

Software Depot

(search for "Standard Mode Security Extensions")

The web page that comes up when you click on the product shows information about the extra features available from this software.

HP-UX - winbindd accesses trusted domains even with 'allow trusted domains' set to 'no'

PROBLEM
With respect to the CIFS Server on an HP-UX 11.x system, winbindd still attempts to access trusted domains even when these two items are in place:

o the smb.conf parameter "allow trusted domains" is set to "no"

o winbind is used to resolve sids to uids/gids in the ADS security model

When these domains are unreachable, winbindd times out and causes problems with authenticating/accessing users in the actual domain that it SHOULD be using.

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - CIFS Server

RESOLUTION
At the time of this writing, winbindd does not currently respect the "allow trusted domains = no" smb.conf parameter. At HP CIFS Server A.02.03 and below, this parameter is only implemented in the smbd daemon.

An enhancement request has been submitted to request that this functionality be added to the winbind daemon in a future release.

HP-UX - root account on Trusted System becomes disabled every few minutes

PROBLEM
The root account on an HP-UX 11.x trusted system becomes disabled about every 5 minutes. This is not a result of malicious activity. PAM debugging was enabled according to the instructions in the following document:

doc_id: UNISKBRC00011843
Title: PAM Debugging
Available at HP's ITRC web site: http://www.itrc.hp.com/

The only interesting entries found in /var/adm/syslog/debug.log were:

```
syslog: unix pam_sm_authenticate(wbem root), flags = 0
syslog: pam_authenticate: error Authentication failed
```

There seem to be several of these grouped together every 5 minutes or so. Could this be causing the root account to get disabled? If so, what is it, and how can I prevent it from disabling the root account?

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - Trusted System

RESOLUTION
Based on the fact that the root account is getting disabled every few minutes along with the fact that the PAM debug entry references wbem root, there is a strong likelihood that this is being caused by another system on the network that is running HP SIM (System Insight Manager). For more information on HP SIM, see the following link: http://h18013.www1.hp.com/products/servers/management/hpsim/index.html

The system that is running SIM is trying unsuccessfully to access the trusted system, and as a result, is causing the root account to be disabled. It is possible that at some time in the past, the SIM system had a legitimate reason to access this trusted system, but for whatever reason, can no longer do so (e.g. the root password on your trusted system has changed).

One way to find the system that is causing this behavior is to enable nettl(1M) tracing to look specifically at the port that is used by HP SIM. See if there is a hint as to where the unsuccessful login originates. In the following steps, assume a source system named Source_1, and a destination system named Dest_1:

1. On the client (Dest_1), start nettl tracing:

nettl -tn all -e all -tm 99999 -f /var/tmp/trace

2. Let this run for about 5 minutes, or until the root account has been disabled. For instance, in another window on system Dest_1, execute "/usr/lbin/getprpw root" until the string "lockout==non-zero" appears.

3. Stop nettl tracing:

nettl -tf -e all

4. Create a filter file in /var/tmp containing the following:

filter ip_daddr Dest_1
filter tcp_dport wbem-https

5. Format the trace file:

netfmt -N -l -c /var/tmp/filter /var/tmp/trace.TRC000 > \
/var/tmp/trace.fmt

6. Edit the trace.fmt file; find a line that mentions system Dest_1 on it, for example:

============= IP Header (inbound -- [ICS]) =============
Source: Source_1.newco.com(A) Dest: Dest_1.newco.com(A)

If it is possible to establish that system Source_1.newco.com is sending requests to the local trusted system, Dest_1.newco.com, then the next step would be to attempt to find out who owns system Source_1 and whether HP SIM was configured to access the trusted system.

For best results with nettl(1M) and netfmt(1M), consider installing the most recent patches for those commands:

o HP-UX 11.11: [PHNE_30450/PACHRDME/English]

Title: nettl(1M), netfmt(1M) and nettladm(1M) patch

o HP-UX 11.23: [PHNE_33283/PACHRDME/English]

Title: nettl(1M), netfmt(1M) and nettladm(1M) patch

Note:
Please apply either of these patches along with any required dependencies. Either of these patches, as with any patch, may be superseded. Please check for the latest patches at HP's IT Resource Center (ITRC) at the following web site:

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

Can HP-UX be attacked by a virus?

PROBLEM
Can HP-UX be attacked by a virus? Is there anti-virus HP-UX software?

RESOLUTION
"Trojans" for UNIX, can exist and would very easy to script. For example: a script that calls /sbin/rm -f /* executed by root will delete the files under / (exception would be /sbin and /sbin/rm and the shell because they are in use). While some people consider trojans a virus, they are not.

A virus has certain characteristics which would define them as a virus. First, a virus is usually memory resident. This means that the virus sits in memory and looks for keys to attack files. Usually the dos extension to the file name, for example .exe files and .com files. Next, a virus must be at least a nuisance, like writing "hacked by chinese" in the case of CodeRed. It also causes an unwanted change to an attacked file. A program that sat in memory and wrote ficticous message to files would be a virus. A virus must also spread itself in one way or another.

Because the virus usually needs a trigger (like the .bat, .exe or some other executable) a UNIX virus is much more difficult to create. Since /usr/bin/rm is an executable not denoted by rm.exe, the virus would not be able to tell by name what is an executable to infect and spread, and what is not. /etc/hosts would look the same to a virus as /etc/ping. A virus would have to be huge to sit in memory and be able to stat all files, run magic, check bits, etc...to know how to spread.

Next, in UNIX the kernel is memory resident. When the system boots the kernel, it is read only. The kernel sits in memory until system shutdown. If a virus was to infect the kernel, it would not be effective until the system was rebooted with the bad kernel. In Win/XXXX the kernel sits on a disk, and is constantly accessed.

The next problem with running a virus in UNIX is that the virus can only run at the access level of the user who executes the program. For example: if johndoe executes the program, the program can only affect johndoe's processes and files. Anything owned by root, and bettysue would be unaffected. The virus could only do wide spread system damage if the super-user root executed the virus. This severely

limits the ability of a virus in UNIX. Windows NT and 2000 also have multi-leveled access for processes, but the implementation is very easy to bypass.

In SunOS and Linux, the virus scanning software that is available is NOT for UNIX/Linux protection, but Microsoft Windows protection. The software is made to scan data shared to and from Windows boxes.

The best defense in UNIX to the Virus threat is common sense, built in UNIX functionality, and basic security measures.

Based on this information, viruses do not pose a threat to a Unix system, where as anyone with root access does. Limit or do not give out root access.

SSH - Do it now

From Bill Hassell

Many of you have heard about SSH but have been reluctant to implement it because it did not come with HP-UX, or because it requires a special terminal emulator. Well, many applications do not come with HP-UX but you can certainly download SSH from HP.

Just go to: software.hp.com or more specifically:

http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

It's free and works on all supported versions of HP-UX. As far as a special terminal emulator, that is true but not an issue. The majority of good commercial terminal emulators such as Reflection (version 10 and later), SecureCRT, EmTec, etc all have SSH capability, and free emulators such as TeraTerm and PuTTY support Secure Shell.

For system administrators, SSH makes the management of multiple systems much easier and safer. You can turn off remsh/rcp/rlogin and rexec and eliminate the security risks with those tools. SSH is also safe for Internet usage; ideal for remote system administration.

Setup for SSH can look very daunting but for the most common implementation (logon and copy files without prompts), it's fairly easy. Basically, you generate two keys on the local machine, and copy the public one to the remote system. There may be a few settings on the remote system to accommodate public key authentication. Start by ensuring that the following settings are uncommented and set like this on each remote system in the /opt/ssh/etc/sshd_config file:

```
Protocol 2
SyslogFacility AUTH
LogLevel INFO
PermitRootLogin yes
HostbasedAuthentication yes
ChallengeResponseAuthentication yes
KerberosAuthentication yes
UsePAM yes
PrintMotd no
EnableSSHKeysign yes
UsePrivilegeSeparation no
Subsystem       sftp    /opt/ssh/libexec/sftp-server
RSAAuthentication yes
DSAAuthentication yes
```

Some of these options may be set already; this is just a checklist. Note: The Secure Shell code is public domain so you may have a different version on your system with different locations for the config files. It is recommended to use the HP compile and packaged version for consistency.

Get a copy from:

http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

Here are the steps to configure one HP-UX system to connect to another. To connect from a PC using a terminal emulator is similar but there are many different packages that support SSH so you'll need to follow your documentation concerning public key generation and the location of the keys. The task list is simple:

1. Generate a public key on the local system.
2. Append the local public key to the remote system's authorized_keys
3. Use SSH to connect from the local system to the remote system

For HP-UX, the steps are these:

1. Logon to the local system

2. Run the command: ssh_keygen -t dsa After running the command, there will be a file called .ssh in your $HOME directory with 2 key files: id_dsa and id_dsa.pub The id_dsa.pub file contains a long key that is exactly one line in length. Now other programs and emulators may add some comments but the key must remain as exactly one line.

3. Now transfer a copy of the id_dsa.pub file to the remote system. Transferring it can take place in a number of ways. You can logon to the remote system, create the directory .ssh in your $HOME directory, and edit the file authorized_keys. If this is the first time you are setting up public keys on this system, it will be a new file. Using vi, edit the authorized_keys file and turn off wrap margin and auto-indent with the command:

```
:set noai wm=0
```

This is important because you don't want vi to split the long line. Now insert the key using copy-paste from the local system's id_dsa.pub files. NOTE: many terminal emulators will insert line break at the right margin of the displayed key. To verify that the text is 1 line, use the $ key in vi to move to the end of the line. If the text is exactly one line then then the cursor will move to the end of the last line. If it moves to the end of the current line, use the J key to join the lines and carefully remove the 1 character that is inserted by vi. Then verify the one line again.

4. Now run SSH from the local system to the remote system. You may get a one-time message to accept the incoming connection. Answer yes and you should be logged in without a login or password request. From now on, you can use scp or sftp to copy files, SSH to run remote commands and even integrate rsync to use SSH for authentication and file transport.

This method provides an excellent authentication method and a secure channel to communicate between machines. The ideal security would be to turn off ftp, telnet, remsh, rlogin, rcp and rexec and just use the Secure Shell for all network communication.

HP Security Bulletins – HP-UX

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00774579

Version: 2

HPSBUX02156 SSRT061236 rev.2 - HP-UX Running Thunderbird, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)

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

Release Date: 2006-09-20

Last Updated: 2007-03-05

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

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

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

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

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

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

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

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
==========
Tbird.TBIRD-COM
->action: install revision 1.5.0.9 or subsequent
->URL: ftp://ftp.mozilla.org/pub/mozilla.org/thunderbird/releases/1.5.0.9/contrib/

END AFFECTED VERSIONS

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

The preliminary versions are available for download from the following url:
ftp://ftp.mozilla.org/pub/mozilla.org/thunderbird/releases/1.5.0.9/contrib/

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

For HP-UX B.11.11 and B.11.23 (PA):

->thunderbird_1.5.0.9_pa.depot.gz
->thunderbird_1.5.0.9_pa.depot.gz.readme

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

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

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

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

PRODUCT SPECIFIC INFORMATION

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

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

HISTORY
Version:1 (rev.1) - 20 September 2006 Initial release
Version:2 (rev.2) - 05 March 2007 preliminary Thunderbird 1.5.0.9 available

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: c00943462

Version: 1

HPSBUX02204 SSRT071341 rev.1 - HP-UX Running CIFS Server (Samba), Remote Denial of Service (DoS)

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

Release Date: 2007-04-02

Last Updated: 2007-04-04

Potential Security Impact: Remote Denial of Service (DoS)

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running CIFS Server (Samba). This vulnerability may allow a remote unauthorized user to create a Denial of Service (DoS).

References: CVE-2007-0452

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP-UX B.11.11, B.11.23, B.11.31 running CIFS Server (Samba)

All versions of HP CIFS Server (Samba) up to and including A.02.03.00 are affected.

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

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

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
==========
CIFS-Server.CIFS-RUN
CIFS-Server.CIFS-UTIL
CIFS-Server.CIFS-ADMIN
CIFS-Server.CIFS-LIB
action: install revision A.02.03.01 or subsequent

END AFFECTED VERSIONS

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

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

HP-UX B.11.11
Install revision A.02.03.01 or subsequent

HP-UX B.11.23
Install revision A.02.03.01 or subsequent

HP-UX B.11.31
Install revision A.02.03.01 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) - 04 April 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.

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00913684

Version: 1

HPSBUX02203 SSRT071339 rev.1 - HP-UX Running Portable File System (PFS), Remote Increase in Privilege

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

Release Date: 2007-03-30

Last Updated: 2007-04-09

Potential Security Impact: Remote increase in privilege.

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in HP-UX with the Portable File System (PFS). The vulnerability could be exploited remotely to gain an increase in privilege.

References: None

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

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

Note: HP-UX B.11.00 is obsolete as of January 1, 2007. It is discussed in this Security Bulletin because the patches cited in the Resolution section were available before January 1, 2007.

As of March 1, 2004 the Portable File System(PFS) is obsolete, and no longer supported on any HP-UX release. PFS is supplied, but no longer supported on HP-UX B.11.00, B.11.11, and B.11.23.

PFS was originally adopted by HP to provide accessibility to Rock Ridge Interchange file system format on CD-ROM file systems. The equivalent functionality is now provided by HP via the HP-UX CDFS file system type and HP-UX's standard file systems commands.

The Hewlett-Packard Company thanks iDefense Labs http://www.idefense.com for reporting this vulnerability to security-alert@hp.com

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

HP-UX B.11.00
==========
OS-Core.CORE-KRN
ProgSupport.C-INC
OS-Core.CORE2-KRN
OS-Core.UX-CORE
action: install PHKL_28060, PHKL_26450, PHCO_26449 or subsequent, discontinue use of PFS.

HP-UX B.11.11
==========
OS-Core.CORE-KRN
ProgSupport.C-INC

OS-Core.CORE2-KRN
OS-Core.UX-CORE
action: PHKL_28025, PHKL_26269, PHCO_25841 or subsequent, discontinue use of PFS.

HP-UX B.11.23
==========
OS-Core.CORE-KRN
ProgSupport.C-INC
OS-Core.CORE2-KRN
OS-Core.UX-CORE
action: discontinue use of PFS.

END AFFECTED VERSIONS

RESOLUTION
The resolution is to avoid the vulnerability by discontinuing the use of PFS.

For B.11.00 and B.11.11, the enhanced CDFS and mount/umount commands are provided by the following patches.

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

HP-UX B.11.00 - PHKL_28060, PHKL_26450, PHCO_26449 or subsequent HP-UX B.11.11 - PHKL_28025, PHKL_26269, PHCO_25841 or subsequent

With these patches, a mount command option (mount -F cdfs -o rr) must be used to enable support of Rock Ridge at mount time.

For B.11.22, B.11.23 and later HP-UX releases, the Rock Ridge Interchange support is provided with the core HP-UX OS and is the default (no patches or special option required).

MANUAL ACTIONS: Yes - NonUpdate
Discontinue the use of PFS.

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) - 09 April 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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00841370

Version: 1

HPSBUX02183 SSRT061243 rev.1 - HP-UX sendmail, Remote Denial of Service (DoS)

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

Release Date: 2007-04-16

Last Updated: 2007-04-17

Potential Security Impact: Remote Denial of Service (DoS)

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running sendmail. This vulnerability could allow a remote user to cause a Denial of Service (DoS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00 (obsolete) running sendmail 8.9.3 or sendmail 8.11.1, HP-UX B.11.11 running sendmail 8.9.3 or sendmail 8.11.1, HP-UX B.11.23 running sendmail 8.11.1.

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

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

For sendmail 8.11.1
HP-UX B.11.23
==========
InternetSrvcs.INETSVCS2-RUN
action: install PHNE_35485 or subsequent

HP-UX B.11.11
==========
SMAIL-UPGRADE.INETSVCS-SMAIL
action: install revision B.11.11.02.004 or subsequent

HP-UX B.11.00
==========
SMAIL-811.INETSVCS-SMAIL
action: remove (use sendmail 8.9.3) or upgrade to HP-UX B.11.11

For sendmail 8.9.3
HP-UX B.11.11
==========
InternetSrvcs.INETSVCS-RUN
action: install PHNE_35484 or subsequent

For sendmail 8.9.3
HP-UX B.11.00
=========
InternetSrvcs.INETSVCS-RUN
action: install PHNE_35483 or subsequent

END AFFECTED VERSIONS

Note:
sendmail 8.13.3 currently available from http://software.hp.com does not exhibit this DoS issue.
sendmail 8.11.1 is no longer available from http://software.hp.com for HP-UX B.11.11; customers are

encouraged to upgrade to sendmail 8.13.3.

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

For sendmail 8.11.1, HP-UX B.11.23
Install: PHNE_35485 or subsequent
sendmail -bs banner: Sendmail 8.11.1 (Revision 1.10)/8.11.1
what(1) string: version.c 8.11.1 (Berkeley) - 01 December 2006
(PHNE_35485)

For sendmail 8.11.1, HP-UX B.11.11
Please write to security-alert@hp.com for more information.

For sendmail 8.11.1, HP-UX B.11.00
Use sendmail 8.9.3 or upgrade to B.11.11 or subsequent. There will be no update to sendmail 8.11.1 for HP-UX B.11.00 to resolve the vulnerability.

For sendmail 8.9.3, HP-UX B.11.11
Install: PHNE_35484 or subsequent
sendmail -bs banner: Sendmail 8.9.3 (Revision 1.10)/8.9.3
what(1) string: version.c 8.9.3 (Berkeley) 01 December 2006 (PHNE_35484)

For sendmail 8.9.3, HP-UX B.11.00
Install: PHNE_35483 or subsequent
sendmail -bs banner: Sendmail 8.9.3 (Revision 1.10)/8.9.3
what(1) string: version.c 8.9.3 (Berkeley) 01 December 2006 (PHNE_35483)

MANUAL ACTIONS: Yes - NonUpdate
HP-UX B.11.11 sendmail 8.11.1 - Write to security-alert@hp.com HP-UX B.11.00 sendmail 8.11.1 - Use sendmail 8.9.3 or upgrade to HP-UX
B.11.11 or subsequent
HP-UX B.11.23 sendmail 8.11.1 - No manual actions HP-UX B.11.11 sendmail 8.9.3 - No manual actions HP-UX B.11.00 sendmail 8.9.3 - No manual actions

PRODUCT SPECIFIC INFORMATION

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

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?_productNumber=B6834AA

HISTORY:
Version: 1 (rev.1) - 16 April 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.

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00944467

Version: 1

HPSBUX02205 SSRT061120 rev.1 - HP-UX Running ARPA Transport, Local Denial of Service (DoS)

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

Release Date: 2007-04-03

Last Updated: 2007-04-09

Potential Security Impact: Local Denial of Service (DoS)

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

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

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00 (obsolete) running ARPA Transport.

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

Note: HP-UX B.11.00 is obsolete as of January 1, 2007. Normally Security Bulletins are not issued for obsolete products. However, the patch cited in the Resolution section was in process before HP-UX B.11.00 became obsolete.

AFFECTED VERSIONS

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

HP-UX B.11.00
==========
OS-Core.CORE2-KRN
Networking.NET-KRN
Networking.NET-PRG
Networking.NET-RUN
Networking.NET2-KRN
Networking.NMS2-KRN
action: install PHNE_35729 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following software patch available to resolve the vulnerability.
This patch is available on: http://itrc.hp.com

HP-UX B.11.00 - PHNE_35729 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) - 9 April 2007 Initial release

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

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

HP-UX SECURITY BULLETIN HPSBUX01137 SSRT5954 rev.10 - HP-UX Running TCP/IP (IPv4), Remote Unauthorized Denial of Service (DoS)

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

Release Date: 2005-04-24

Last Updated: 2007-04-25

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 running TCP/IP (IPv4). This vulnerability could be remotely exploited by an unauthorized user to cause a Denial of Service (DoS).

References: CAN-2005-1192

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.22, B.11.23.

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

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

AFFECTED VERSIONS

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

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

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

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN
action: install revision A.01.07.02 and PHNE_33159 or subsequent

HP-UX B.11.11
==========
IPSec.IPSEC2-KRN
action: install revision A.02.00.01 and TOUR 3.0

HP-UX B.11.23
==========
IPSec.IPSEC2-KRN
action: install revision A.02.00.01 and PHNE_32606 or subsequent

HP-UX B.11.23
==========
IPSec.IPSEC2-KRN
action: install revision A.02.00.01 and TOUR 3.0

END AFFECTED VERSIONS

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

Previous revisions of this Security Bulletin recommended setting ip_pmtu_strategy to 0 or 3 as a workaround. Patches or updates to resolve the issue are now available. After these patches or updates are installed the workaround will no longer be necessary or recommended.
->The ip_pmtu_strategy parameter should be restored to the default value of 1.

->Note: Previous versions of this Security Bulletin incorrectly stated that the default value of ip_pmtu_strategy is 2.

RESOLUTION
Patches are available for the core TCP/IP product for B.11.11 and B.11.23 from:

http://itrc.hp.com

For B.11.11 - PHNE_33159 or subsequent
For B.11.23 - PHNE_32606 or subsequent

Binary files are available for B.11.22 as discussed in Security Bulletin HPSBUX01164.

Patches and updates are available for IPSec.

The patches are available from http://itrc.hp.com IPSec and TOUR (Transport Optional Upgrade Release) are available from http://www.hp.com/go/softwaredepot

For B.11.11 IPSec:
IPSec revision A.01.07.02 and PHNE_33159 or subsequent or IPSec revision A.01.07.02 and TOUR 3.0

For B.11.23 IPSec:
IPSec revision A.02.00.01 and PHNE_32606 or subsequent or IPSec revision A.02.00.01 and TOUR 3.0

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

B11.11 running IPSec
Install IPSec revision A.01.07.02 and PHNE_33159 or subsequent or Install IPSec revision A.01.07.02 and TOUR 3.0

B11.23 running IPSec
Install IPSec revision A.02.00.01 and PHNE_32606 or subsequent or Install IPSec revision A.02.00.01 and TOUR 3.0

PRODUCT SPECIFIC INFORMATION

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

For more information see:

https://www.hp.com/go/swa

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

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: c00819543

Version: 1

HPSBMA02197 SSRT061285 rev.1 - HP-UX Running HP Power Manager Remote Agent (RA), Local Execution of Arbitrary Code with Root Privileges

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

Release Date: 2007-04-25

Last Updated: 2007-04-25

Potential Security Impact: Local execution of arbitrary code with root privileges

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running HP Power Manager Remote Agent (RA). The vulnerability could be exploited by a local authorized user to execute arbitrary code with the privileges of the root user.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23 running HP Power Manager RA revision 4.0Build10 and previous.

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

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

AFFECTED VERSIONS

HP-UX B.11.23
HP-UX B.11.11
==========
HPPowerManagerRA.exec,r<=4.0Build10
action: install HPPowerManagerRA revision 4.0Build11 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has provided the following software update to resolve this vulnerability:

HP Power Manager (HPPM) - HPUX Remote Agent - HPPowerManagerRA revision 4.0Build11 or subsequent

The update is available for download from:

http://h18004.www1.hp.com/products/servers/proliantstorage/power-protection/software/power-manager/pm3-dl.html

The update is provided as a tar archive:
HP Power Manager (HPPM) - HPUX Remote Agent (tar)

Further information can be found in the HP-UXReadme.txt file in the tar archive.

MANUAL ACTIONS: Yes - Update
Update to HPPowerManagerRA revision 4.0Build11 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) 25 April 2007 Initial release

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

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

HP Security Bulletins – Tru64

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00967144

Version: 1

HPSBTU02207 SSRT061213, SSRT061239, SSRT071304 rev.1 - HP Tru64 UNIX SSL and BIND 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: 2007-04-12

Last Updated: 2007-04-12

Potential Security Impact: Remote unauthenticated arbitrary code execution or Denial of Service (DoS)

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified on the Secure Sockets Layer (SSL) and BIND running on the HP Tru64 UNIX Operating System that may allow a remote attacker to execute arbitrary code or cause a Denial of Service (DoS).

References: VU#547300, VU#386964, CAN-2006-4339, CVE-2006-2937, CVE-2006-2940, CVE-2006-3738 (SSL) VU#697164, VU#915404, CVE-2007-0493, CVE-2007-0494 (BIND)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected:

HP Tru64 UNIX v 5.1B-4 (SSL and BIND)
HP Tru64 UNIX v 5.1B-3 (SSL and BIND)
HP Tru64 UNIX v 5.1A PK6 (BIND)
HP Tru64 UNIX v 4.0G PK4 (BIND)
HP Tru64 UNIX v 4.0F PK8 (BIND)
Internet Express (IX) v 6.6 BIND (BIND) HP Insight Management Agents for Tru64 UNIX patch v 3.5.2 and earlier(SSL)

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

RESOLUTION
HP has released the following Early Release Patch kits (ERPs) publicly for use by any customer. The ERP kits use dupatch to install and will not install over any Customer Specific Patches (CSPs) that have file intersections with the ERP. A new patch version for HP Insight Management Agents for Tru64 UNIX is also available that addresses the potential vulnerabilities.

The fixes contained in the ERP kits will be available in the following mainstream releases:

Targeted for availability in HP Tru64 UNIX v 5.1B-5 Internet Express (IX) v 6.7 HP Insight Management Agents for Tru64 UNIX patch v 3.6.1 (already available)

HP Tru64 UNIX Version 5.1B-4 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001167-V51BB27-ES-20070321

Name: T64KIT1001167-V51BB27-ES-20070321

MD5 Checksum: a697a90bd0b1116b6f27d1100bbf81fd

HP Tru64 UNIX Version 5.1B-3 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001163-V51BB26-ES-20070315

Name: T64KIT1001163-V51BB26-ES-20070315

MD5 Checksum: d376d403176f0dbe7badd4df4e91c126

HP Tru64 UNIX Version 5.1A PK6 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001160-V51AB24-ES-20070314

Name: T64KIT1001160-V51AB24-ES-20070314

MD5 Checksum: 7bb43ef667993f7c4711b6cf978e0aa7

HP Tru64 UNIX Version 4.0G PK4 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001166-V40GB22-ES-20070316

Name: T64KIT1001166-V40GB22-ES-20070316

MD5 Checksum: a446c39169b769c4a03c654844d5ac45

HP Tru64 UNIX Version 4.0F PK8 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1001165-V40FB22-ES-20070316

Name: DUXKIT1001165-V40FB22-ES-20070316

MD5 Checksum: 718148c87a913536b32a47af4c36b04e

HP Insight Management Agents for Tru64 UNIX patch version 3.6.1 (for kit CPQIIM360)

Location: http://h30097.www3.hp.com/cma/patches.html

Name: CPQIM360.SSL.01.tar.gz

MD5 Checksum: 1001a10ab642461c87540826dfe28652

Internet Express (IX) v 6.6 BIND

Note: Customers who use Internet Express (IX) v 6.6 BIND should install the BIND 9.2.8 patch from the ERP kit appropriate for their base operating system version.

PRODUCT SPECIFIC INFORMATION

The HP Tru64 UNIX v 5.1B-3 and v 5.1B-4 ERP kits distribute two patches:

OpenSSL 0.9.8d
BIND 9.2.8 built with OpenSSL 0.9.8d

Note: HP Tru64 UNIX v 5.1A, v 4.0G, and v 4.0F releases did not distribute OpenSSL and so their ERP kits provide only the BIND 9.2.8 patch that has been built with OpenSSL 0.9.8d

Customers who have been using OpenSSL on HP Tru64 UNIX v 5.1B-3 and v 5.1B-4 should install the OpenSSL patch from the ERP kit appropriate for their base operating system version.

The HP Insight Management Agents for Tru64 UNIX patch contains OpenSSL 0.9.8d and is applicable for HP Tru64 UNIX v 5.1A, v 5.1B-3, and v 5.1B-4.

HISTORY

Version:1 (rev.1) - 12 April 2007 Initial release

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

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

HP TRU64 SECURITY BULLETIN

HPSBTU02179 SSRT061256 rev.1 - HP Tru64 UNIX Running the ps command, Local Disclosure of Sensitive Information

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

Release Date: 2007-04-25

Last Updated: 2007-04-25

Potential Security Impact: Local disclosure of sensitive information

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with the HP Tru64 UNIX Operating System running the ps command. The ps command could be used to disclose information about a process's arguments and environmental variables that might be exploited by a local, authorized user.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected:

HP Tru64 UNIX v5.1B-4
HP Tru64 UNIX v5.1B-3
HP Tru64 UNIX v5.1A PK6
HP Tru64 UNIX v4.0G PK4
HP Tru64 UNIX v4.0F PK8

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

RESOLUTION
HP has released the following Early Release Patch kits (ERPs) publicly for use by any customer.

The ERP kits use dupatch to install and will not install over any Customer Specific Patches (CSPs) that have file intersections with the ERP.

The resolutions contained in the ERP kits are targeted for availability in the following mainstream patch kit:

HP Tru64 UNIX Version v5.1B-5

The ERP kits distribute the following files:

/usr/bin/ps
/sbin/ps

After installing the patch kit, by default, the HP Tru64 UNIX ps command behaves just the same: it can display a process's arguments, and the ps e command displays a process's environmental variables.

To prevent users from seeing the arguments and environmental variables of other users, set new variables in the "/etc/rc.config.common" file (versions v5.1A PK6, v5.1B-3, v5.2B-4) or the "/etc/rc.config" file (versions v4.0G PK4 and v4.0F PK8) as follows:

For HP Tru64 UNIX versions v5.1B-4, v5.1B-3 and v5.1A PK6, use:

rcmgr -c set TBL_ARGUMENTS_DISABLE 1
rcmgr -c set TBL_ENVIRONMENT_DISABLE 1

For HP Tru64 UNIX versions v4.0G PK4 and v4.0F PK8, use:

rcmgr set TBL_ARGUMENTS_DISABLE 1
rcmgr set TBL_ENVIRONMENT_DISABLE 1

Important notes about setting these new variables:

Setting the new variables to prevent the ps command from allowing non-root users to display other users arguments and environment variables might cause some applications or program scripts to not function properly. The root user running the ps command will continue to be allowed to display other users arguments and environment variables.

HP Tru64 UNIX Version v5.1B-4 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001143-V51BB27-ES-20070305

Name: T64KIT1001143-V51BB27-ES-20070305

MD5 Checksum: 44b15d10895cf0606003a572b3310f9a

HP Tru64 UNIX Version v5.1B-3 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001144-V51BB26-ES-20070305

Name: T64KIT1001144-V51BB26-ES-20070305

MD5 Checksum: 67cfabb7cd3c422e2dc6bb6ed3d7d290

HP Tru64 UNIX Version v5.1A PK6 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001145-V51AB24-ES-20070305

Name: T64KIT1001145-V51AB24-ES-20070305

MD5 Checksum: de6885b166dba703af862ce05431e5cc

HP Tru64 UNIX Version v4.0G PK4 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001179-V40GB22-ES-20070330

Name: T64KIT1001179-V40GB22-ES-20070330

MD5 Checksum: 31129e60bb01ffdea015312c0e019fae

HP Tru64 UNIX Version v4.0F PK8 ERP Kit

Location:
http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1001180-V40FB22-ES-20070330

Name: DUXKIT1001180-V40FB22-ES-20070330

MD5 Checksum: db9d634bb27f02642e00f149d6ebb8ee

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

Third Party Security Patches: Third party security patches which are to be installed on systems

running HP software products should be applied in accordance with the customer's patch management policy.

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

HP TRU64 SECURITY BULLETIN

HPSBTU02116 SSRT061135 rev.3 - HP Tru64 UNIX and HP Internet Express for Tru64 UNIX Running sendmail, Remote Execution of Arbitrary Code or Denial of Service (DoS)

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

Release Date: 2007-04-25

Last Updated: 2007-04-25

Potential Security Impact: Remote execution of arbitrary code, Denial of Service (DoS)

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP Tru64 UNIX or HP Internet Express for Tru64 UNIX running sendmail which may allow a remote attacker to execute arbitrary code or cause a Denial of Service (DoS).

References: CVE-2006-0058 (VU#834865), CVE-2006-1173 (VU#146718)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. The following supported software versions are affected:

HP Tru64 UNIX v5.1B-3
HP Tru64 UNIX v5.1B-2/PK4
HP Tru64 UNIX v5.1A PK6
HP Tru64 UNIX v4.0G PK4
HP Tru64 UNIX v4.0F PK8
HP Internet Express for Tru64 UNIX v6.3
HP Internet Express for Tru64 UNIX v6.4
HP Internet Explorer for Tru64 UNIX v6.5

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

RESOLUTION
HP has released the following Early Release Patch kits (ERPs) publicly for use by any customer.

The ERP kits use dupatch to install and will not install over any Customer Specific Patches (CSPs) that have file intersections with the ERP.

The resolutions contained in the ERP kits are targeted to be available in the following supported patch kits:

Tru64 UNIX v5.1B-4

The ERP kits distribute sendmail 8.13.6.

HP Tru64 UNIX Version v5.1B-3 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001125-V51BB26-ES-

20070220

Name:T64KIT1001125-V51BB26-ES-20070220

MD5 Checksum: bd43eb3b99466a9d82d01c1f5cc33f9c

HP Tru64 UNIX Version v5.1B-2/PK4 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1000617-V51BB25-ES-20060515

Name: T64KIT1000617-V51BB25-ES-20060515

MD5 Checksum: 1d8a0dc34628b5898c99b6dab2714320

HP Tru64 UNIX Version v5.1A PK6 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1000618-V51AB24-ES-20060515

Name: T64KIT1000618-V51AB24-ES-20060515

MD5 Checksum: b9a2ef1d0c1745ce0fa265b2d2fd8c32

HP Tru64 UNIX Version v4.0G PK4 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1000635-V40GB22-ES-20060519

Name: T64KIT1000635-V40GB22-ES-20060519

MD5 Checksum: 2c74941543d969c92adef38a44b5c764

HP Tru64 UNIX Version v4.0F PK8 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1000636-V40FB22-ES-20060519

Name: DUXKIT1000636-V40FB22-ES-20060519

MD5 Checksum: 9735ad5cc5c705e8bbbbefb01feb4128

HP Internet Express for Tru64 UNIX v6.3 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64V51AB-IX-631-SENDMAIL-SSRT-061135

Name: T64V51AB-IX-631-SENDMAIL-SSRT-061135

MD5 Checksum: ee9e7d5b0cc01e0424edc05021670820

HP Internet Express for Tru64 UNIX v6.4 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64V51AB-IX-641-SENDMAIL-SSRT-061135

Name: T64V51AB-IX-641-SENDMAIL-SSRT-061135

MD5 Checksum: 5b1a544575a62831c173fc489b8eaeea

HP Internet Explorer for Tru64 UNIX v6.5 ERP Kit

Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64V51AB-IX-651-SENDMAIL-SSRT-061135

Name: T64V51AB-IX-651-SENDMAIL-SSRT-061135

MD5 Checksum: 0b6268159a9957c56ff2f35cea2057d8

PRODUCT SPECIFIC INFORMATION

HISTORY

Version: 1 (rev.1) 5 June 2006 Initial release
Version: 2 (rev.2) 15 June 2006 Updated references
Version: 3 (rev.3) 25 April 2007 Updated to add new ERP kit for HP Tru64 UNIX v5.1B-3 because PSM functionality was broken in the HPSBTU02116 rev.2 ERP kit T64KIT1000619-V51BB26-ES-20060515

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

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01036871

Version: 1

HPSBTU02211 SSRT071326 rev.1 - HP Tru64 UNIX Running the dop command, Local Execution of Arbitrary Code with Privilege Elevation

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

Release Date: 2007-05-01

Last Updated: 2007-05-01

Potential Security Impact: Local execution of arbitrary code with privilege elevation

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with the HP Tru64 UNIX Operating System running the dop command. The vulnerability could be exploited by a local, authorized user to execute arbitrary code with the privileges of the root user.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions are affected:

HP Tru64 UNIX v5.1B-4
HP Tru64 UNIX v5.1B-3
HP Tru64 UNIX v5.1A PK6

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

The Hewlett-Packard Company thanks Daniele Calore for reporting this vulnerability to security-alert@hp.com

RESOLUTION
Until updates are available in mainstream release patch kits, HP is releasing the following Early Release Patch (ERP) kits publicly for use by any customer.

The ERP kits use dupatch to install and will not install over any installed Customer Specific Patches (CSPs) that have file intersections with the ERPs. Contact your service provider for assistance if the installation of the ERPs is blocked by any of your installed CSPs.

The resolutions contained in the ERP kits are targeted for availability in the following mainstream patch kit:

HP Tru64 UNIX Version v5.1B-5

HP Tru64 UNIX Version v5.1B-4
PREREQUISITE: HP Tru64 UNIX v5.1B-4 PK6 (BL27)
Name: T64KIT1001178-V51BB27-E-20070330
Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001188-V51BB27-ES-20070404

HP Tru64 UNIX Version v5.1B-3
PREREQUISITE: HP Tru64 UNIX v5.1B-3 PK5 (BL26)
Name: T64KIT1001189-V51BB26-ES-20070405
Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001189-V51BB26-ES-20070405

HP Tru64 UNIX Version v5.1A
PREREQUISITE: HP Tru64 UNIX v5.1A PK6 (BL24)
Name: T64KIT1001190-V51AB24-ES-20070405
Location:
http://www2.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001190-V51AB24-ES-20070405

MD5 checksums are available from the ITRC patch database main page. From the patch database main page, click Tru64 UNIX, then click verifying MD5 checksums under useful links.

PRODUCT SPECIFIC INFORMATION

HISTORY

Version 1 (rev.1) - 1 May 2007 Initial release

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

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

HP Security Bulletin – ProCurve

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01034753

Version: 2

HPSBMI02210 SSRT071396 rev.2 - 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: 2007-05-09

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: none

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

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) - 25 April 2007 Initial release

Version: 2 (rev.2) - 09 May 2007 Updated resolution due to 08.0.01k update available now, changed recommendation from v07.08.03 to v08.0.01k

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

HP Security Bulletins – OpenView

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00727143

Version: 4

HPSBMA02133 SSRT061201 rev.4 - 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: 2007-04-18

Potential Security Impact: Local or remote compromise of confidentiality, availability, integrity.
Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
Oracle(r) has issued a Critical Patch Update which contains solutions for a number of potential security vulnerabilities. These vulnerabilities may be exploited locally or remotely to compromise the confidentiality, availability or integrity of Oracle for OpenView (OfO).

References: Oracle Critical Patch Update - April 2007

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
Oracle for OpenView (OfO) v8.1.7 or v9.1.01 or v9.2 running on HP-UX, Tru64 UNIX, Linux, Solaris, and Windows.

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

Oracle has issued Critical Patch Update - April 2007.

For more information:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

Information about previous Oracle Critical Patch Updates can be found here:
http://www.oracle.com/technology/deploy/security/alerts.htm

The following products are affected:

Product Number
  Description

ORA200BC
  OfO v8.1.7 for HP-UX LTU

ORA200CA
  OfO v9.2 64bit HP-UX 11&11.11 LTU

ORA205BC
  OfO v8.1.7 for HP-UX 5 LTU Bundle

ORA205CA
  OfO v9.2 64bit HP-UX 11&11.11 5 LTUs

ORA230BC
  OfO v8.1.7 for HP-UX Media

ORA230CA
  OfO v9.2 64bit HP-UX 11&11.11 Media Kit

ORA240BC
  OfO v8.1.7 for HP-UX Eval LTU & Media

ORA300BC
  OfO v8.1.7 for Win 2000/NT LTU

ORA300CA
  OfO v9.2 32bit Windows LTU

ORA305BC
  OfO v8.1.7 for Win 2000/NT 5 LTU Bundle

ORA305CA
OfO v9.2 32bit Windows 5 LTUs

ORA330BC
OfO v8.1.7 for Win 2000/NT Media

ORA330CA
OfO v9.2 32bit Windows Media Kit

ORA340BC
OfO v8.1.7 for Win 2000/NT Eval LTU

ORA400BC
OfO v8.1.7 for Sun Solaris LTU

ORA400CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 LTU

ORA401CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 LTU

ORA405BC
OfO v8.1.7 for Sun Solaris 5 LTU Bundle

ORA405CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 5 LTU

ORA406CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 5 LTU

ORA430BC
OfO v8.1.7 for Sun Solaris Media

ORA430CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 Media

ORA431CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 Media

ORA440BC
OfO v8.1.7 for Sun Solaris Eval LTU

ORA500CA
OfO v9.1.01 64bit Tru64 V5.1a LTU Ent.Ed

ORA505CA
OfO v9.1.01 64bit Tru64 V5.1a LTU

ORA530CA
OfO v9.1.01 64bit Tru64 V5.1a Media Kit

ORA600CA
OfO for Linux LTU

ORA605CA
OfO for Linux LTU Service Bureaus Bundle

ORA630CA
OfO v9.2.0 for Linux, Media Kit

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
==========
action: If Oracle for OpenView (OfO) is installed, install the Oracle Critical Patch Update - April 2007

END AFFECTED VERSIONS

Note: Since Oracle for OpenView (OfO) is not installed using swinstall(1M) the Security Patch Check Tool cannot determine whether it is present on an HP-UX system. Customer maintained configuration documentation should be consulted to determine whether Oracle for OpenView (OfO) is installed.

RESOLUTION
Oracle for OpenView (OfO) customers who have support contracts directly with Oracle should obtain the "Critical Patch Update - April 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 - April 2007."

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

MANUAL ACTIONS : Yes - Update
Install the Oracle Critical Patch Update - April 2007.

Oracle is a registered U.S. trademark of the Oracle Corporation, Redwood City, California.

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

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: c00742778

Version: 3

HPSBMA02138 SSRT061184 rev.3 - HP OpenView Storage Data Protector, Remote Unauthorized Arbitrary Command Execution

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

Release Date: 2006-08-10
Last Updated: 2007-04-30

Potential Security Impact: Remote unauthorized arbitrary command execution

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP OpenView Storage Data Protector running on HP-UX, IBM AIX, Linux, Microsoft Windows, and Solaris. This vulnerability could allow a remote unauthorized user to execute arbitrary commands.

References: NISCC 412866

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Storage Data Protector 5.1 and 5.5 running on HP-UX, IBM AIX, Linux, Microsoft Windows, and Solaris.

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

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

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

AFFECTED VERSIONS

For HP OpenView Storage Data Protector 5.1

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
==========
DATA-PROTECTOR.OMNI-CORE
action: install PHSS_34887 or subsequent, deploy to client systems

For HP OpenView Storage Data Protector 5.5

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
==========
DATA-PROTECTOR.OMNI-CORE
action: install PHSS_35142 or subsequent, deploy to client systems

HP-UX B.11.23 (IA)
==========
DATA-PROTECTOR.OMNI-CORE
action: install PHSS_35143 or subsequent, deploy to client systems

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve the issue.

The patches can be downloaded from: http://itrc.hp.com

The HP-UX patches listed are applied to Installation Servers. They contain the updates for HP-UX, IBM AIX, and Linux clients. More information can be found in the Special Installation Instructions section of the patch documentation.

HP OpenView Storage Data Protector 5.1

For HP-UX, IBM AIX, and Linux
PHSS_34887 or subsequent - B.11.00, B.11.11, B.11.23 (PA) Installation Servers

For Solaris
DPSOL_00204 or subsequent

For Windows
DPWIN_00206 or subsequent

HP OpenView Storage Data Protector 5.5

->For HP-UX, IBM AIX, and Linux (except for x86_64)
PHSS_35142 or subsequent - B.11.00, B.11.11, B.11.23 (PA) Installation Servers
PHSS_35143 or subsequent - B.11.23 (IA) Installation Servers

->For Linux x86_64
->Install SSPUX550_159 and its prerequisite patches SSPUX550_068 and SSPUX550_069.

These patches will be available via the following ftp site until June 1, 2007. After that date the patches will be available by contacting HP Support.

System: hprc.external.hp.com (192.170.19.100)
Login: ss061184
Password: ss061184 (NOTE: CASE-sensitive)

ftp://ss061184:ss061184@192.170.19.100/

SSPUX550_159.shar.gz
SSPUX550_068.shar.gz
SSPUX550_069.shar.gz

md5sum: (SSPUX550_159.shar) = 813c8ff5281af853040bc6f6a6339f8a
md5sum: (SSPUX550_068.shar) = f3f523262cce6523e0e11605cd06de6b
md5sum: (SSPUX550_069.shar) = c3841b88e496e38bd8e2b7baa0b5d545

cksum: 1893672450 7239656 SSPUX550_068.shar
cksum: 2719159727 3594346 SSPUX550_069.shar
cksum: 19364427 269610 SSPUX550_159.shar

For Solaris
DPSOL_00228 or subsequent

For Windows
DPWIN_0202 or subsequent

MANUAL ACTIONS: Yes - Non-HP-UX only
For HP OpenView Storage Data Protector 5.5 Linux x86_64 Download and install SSPUX550_159 and its prerequisite patches
SSPUX550_068 and SSPUX550_069

PRODUCT SPECIFIC INFORMATION

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

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

HISTORY:
Version: 1 (rev.1) - 10 August 2006 Initial release
Version: 2 (rev.2) - 25 October 2006 Patches available
Version: 3 (rev.3) - 30 April 2007 Linux x86_64 patches available

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

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

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00854999

Version: 1

HPSBMA02198 SSRT061177 rev.1 - HP OpenView Network Node Manager (OV NNM) Remote Unauthorized Access

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

Release Date: 2007-03-21

Last Updated: 2007-03-21

Potential Security Impact: Remote unauthorized access

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

VULNERABILITY SUMMARY
A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM). This vulnerability could be exploited remotely to gain unauthorized access to certain facilities of the NNM server.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP OpenView Network Node Manager (OV NNM) 6.20, 6.4x, 7.01, 7.50, 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.

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

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

AFFECTED VERSIONS

For HP-UX OV NNM 7.50 and 7.51
HP-UX B.11.23 (IA)
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_35844 or subsequent

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_35843 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_35579 or subsequent

For HP-UX OV NNM 6.4x
HP-UX B.11.00
HP-UX B.11.11
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_34949 or subsequent

For HP-UX OV NNM 6.20
HP-UX B.11.00
HP-UX B.11.11
==========
OVNNMgr.OVNNM-RUN
action: install PHSS_35113 or subsequent

For Solaris OV NNM 7.50 and 7.51
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
==========
action: install PSOV_03470 or subsequent

For Solaris OV NNM 7.01
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
==========
action: install PSOV_03468 or subsequent

For Solaris OV NNM 6.4x
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
==========
action: install PSOV_03460 or subsequent

For Solaris OV NNM 6.20
SunOS 5.6
SunOS 5.7

SunOS 5.8
SunOS 5.9
==========
action: install PSOV_03461 or subsequent

For Windows OV NNM 7.50 and 7.51
Windows NT
Windows 2000
Windows XP
==========
action: install NNM_01149 or subsequent

For Windows OV NNM 7.01
Windows NT
Windows 2000
Windows XP
==========
action: install NNM_01147 or subsequent

For Windows OV NNM 6.4x
Windows NT
Windows 2000
Windows XP
==========
action: install NNM_01138 or subsequent

For Windows OV NNM 6.20
Windows NT
Windows 2000
Windows XP
==========
action: install NNM_01139 or subsequent

For Linux OV NNM 7.50 and 7.51
Linux RedHatAS2.1
==========
action: install LXOV_00050 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has provided the following patches to resolve this potential vulnerability.
These patches are available from http://support.openview.hp.com/patches/

OpenView Network Node Manager 7.50 and 7.51

HP-UX B.11.23 (IA)
  PHSS_35844 or subsequent

HP-UX B.11.23 (PA)
  PHSS_35843 or subsequent

HP-UX B.11.11
  PHSS_35843 or subsequent

HP-UX B.11.00

PHSS_35843 or subsequent

Linux RedHatAS2.1
LXOV_00050 or subsequent

Solaris
PSOV_03470 or subsequent

Windows
NNM_01149 or subsequent

OpenView Network Node Manager 7.01

HP-UX B.11.11
PHSS_35579 or subsequent

HP-UX B.11.00
PHSS_35579 or subsequent

Solaris
PSOV_03468 or subsequent

Windows
NNM_01147 or subsequent

OpenView Network Node Manager 6.4x

HP-UX B.11.11
PHSS_34949 or subsequent

HP-UX B.11.00
PHSS_34949 or subsequent

Solaris
PSOV_03460 or subsequent

Windows
NNM_01138 or subsequent

OpenView Network Node Manager 6.20

HP-UX B.11.11
PHSS_35113 or subsequent

HP-UX B.11.00
PHSS_35113 or subsequent

Solaris
PSOV_03461 or subsequent

Windows
NNM_01139 or subsequent

MANUAL ACTIONS: Non-HP-UX only
Install the patches listed in the Resolution section for Solaris, Windows NT, Windows 2000, Windows XP, 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) - 21 March 2007 Initial release

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

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

HP Security Bulletin – JetDirect

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00838612

Version: 2

HPSBPI02185 SSRT071290 rev.2 - HP Jetdirect Running ftp, Remote Denial of Service (DoS)

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

Release Date: 2007-01-17

Last Updated: 2007-04-25

Potential Security Impact: Remote Denial of Service (DoS)

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

VULNERABILITY SUMMARY
A potential vulnerability has been identified with HP Jetdirect running ftp. The vulnerability could be exploited remotely to create a Denial of Service (DoS).

References: CVE-2007-1772

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Jetdirect running firmware versions from x.20.nn up to and including x.24.nn

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

->Note: The resolution below addresses the vulnerability reported in CVE-2007-1772.

The whitepaper 'HP Jetdirect Security Guidelines' has recommendations for securing HP Jetdirect.

The whitepaper is available here:
http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00746792/c00746792.pdf

RESOLUTION
This vulnerability can be resolved by upgrading the Jetdirect firmware. There is also a workaround for this vulnerability by making configuration changes.

Recent Jetdirect products use firmware revision x.25.nn or greater and are not vulnerable. Some older Jetdirect products allow the firmware to be upgraded and others do not.

Instructions for upgrading Jetdirect firmware are available here:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07429

For J4169A 610n - upgrade the firmware to version L.25.nn or greater.

For J6057A 615n - upgrade the firmware to version R.25.nn or greater.

Other older Jetdirect products running versions from x.20.nn up to and including x.24.nn are potentially vulnerable. The firmware for these products cannot be upgraded. The potential vulnerability can be avoided by disabling ftp or using access control lists as discussed in the whitepaper 'HP Jetdirect Security Guidelines' mentioned above.

PRODUCT SPECIFIC INFORMATION

HISTORY
Version:1 (rev.1) - 17 January 2007 Initial release
Version:2 (rev.2) - 25 April 2007 Added reference to CVE-2007-1772

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 – ServiceGuard

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00860750

Version: 3

HPSBGN02189 SSRT071297 rev.3 - ServiceGuard for Linux, Remote Unauthorized Access

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

Release Date: 2007-02-12

Last Updated: 2007-05-07

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 Serviceguard for Linux that may allow remote unauthorized access.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP Serviceguard for Linux:

->RedHat 7.3 / Enerprise Linux 2.1, prior to release SG A.11.14.06
SuSE SLES8 United Linux 1.0, prior to release SG A.11.15.07 SuSE SLES9 SLES10, prior to release SG A.11.16.10

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

RESOLUTION

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

Retrieve applicable patches and install using applicable Linux tools.

SuSE SLES8 United Linux 1.0, release SG A.11.15.07

SLES8/UL1.0 IA32 SGLX_00070
SLES8/UL1.0 IA64 SGLX_00071

SuSE SLES9 SLES10, release SG A.11.16.10

SLES9 IA32 SGLX_00114
SLES9 IA64 SGLX_00115
SLES9 x86_64 SGLX_00116

SLES10 IA32 SGLX_00117
SLES10 IA64 SGLX_00118
SLES10 x86_64 SGLX_00119

->RedHat 7.3, Enterprise Linux 2.1, release SG A.11.14.06

->RedHat 7.3 RedHat2.1AS Redhat2.1ES IA32 SGLX_00120

RedHat Enterprise Linux, release SG A.11.16.10

RedHat3.0AS RedHat3.0ES IA32 SGLX_00099
RedHat3.0AS RedHat3.0ES IA64 SGLX_00100
RedHat3.0AS RedHat3.0ES x86_64 SGLX_00101

RedHat4AS RedHat4ES IA32 SGLX_00111
RedHat4AS RedHat4ES IA64 SGLX_00112
RedHat4AS RedHat4ES x86_64 SGLX_00113

PRODUCT SPECIFIC INFORMATION

HISTORY
Version: 1 (rev.1) - 12 February 2007 Initial release
Version: 2 (rev.2) - 05 March 2007 Corrected title typo
Version: 3 (rev.3) - 07 May 2007 Added SG 11.14.06 patch

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 Storageworks Command View

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00911797

Version: 1

HPSBST02200 SSRT071330 rev.1 - HP StorageWorks Command View Advanced Edition for XP, Local Unauthorized Access

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

Release Date: 2007-03-28

Last Updated: 2007-04-03

Potential Security Impact: Local unauthorized access

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

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP StorageWorks Command View Advanced Edition for XP software where new user registration or addition may allow local unauthorized access to user accounts.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP StorageWorks Command View Advanced Edition for XP v 5.0.0-00 to v 5.1.0-05 and v 5.5.0 -00 to v 5.5.0-02

HP StorageWorks XP Replication Monitor v 1.1.0-00 and v 5.0.0-00 to v 5.5.0-02

HP StorageWorks XP Tiered Storage Manager v 1.1.0-00 and v 5.0.0-00 to v 5.5.0-01

When at least one of the following Lines/Models is installed on a single server:

HP StorageWorks Command View Device Manager HP StorageWorks Command View Global Link Availability Manager HP StorageWorks Command View Replication Monitor HP StorageWorks Command View Tiered Storage Manager HP StorageWorks Command View Tuning Manager

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

RESOLUTION
HP has made the following software updates available to resolve this issue. The updates are available via the following Web page:

http://welcome.hp.com/country/us/en/support.html?pageDisplay=drivers

HP StorageWorks Command View Advanced Edition for XP Install v 5.6.0-01 or subsequent HP StorageWorks XP Replication Monitor Install v 5.6.0-01 or subsequent

HP StorageWorks XP Tiered Storage Manager Install v 5.5.0-02 or subsequent

Note: Delete or change the user authentication information for all user accounts after updated software versions are installed.

PRODUCT SPECIFIC INFORMATION

HISTORY
Version: 1 (rev.1) - 03 April 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.

Microsoft Security Bulletins – Storage Management Appliance (SMA)

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00965724

Version: 2

HPSBST02206 SSRT071354 rev.2 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-017

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

Release Date: 2007-04-10

Last Updated: 2007-04-17

Potential Security Impact: Please check the table below

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

VULNERABILITY SUMMARY
Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-017

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

MS07-017 Vulnerabilities in GDI Could Allow Remote Code Execution (925902)
Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

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) - 10 April 2007 Initial release
Version: 2 (rev.2) - 17 April 2007 Corrected MS patch # MS07-014 to MS07-017

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: c00978780

Version: 1

HPSBST02208 SSRT071365 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-018 to MS07-022

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

Release Date: 2007-04-18

Last Updated: 2007-04-18

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: MS07-018, MS07-019, MS07-020, MS07-021, MS07-022.

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

MS07-018

Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution (925939) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-019

Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-020

Vulnerability in Microsoft Agent Could Allow Remote Code Execution
(932168)
Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-021

Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178) Possible security issue exists.

Patch will run successfully.
  For SMA v2.1, customers should download patch from Microsoft and install.

MS07-022

Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)
  Possible security issue exists.

Patch will run successfully.
  For SMA v2.1, customers should download patch from Microsoft and install.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

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) - 18 April 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.

Security Bulletin – Miscellaneous

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c00901872

Version: 1

HPSBGN02199 SSRT071312 rev.1 - Mercury Quality Center ActiveX, Remote Unauthorized Arbitrary Code Execution

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

Release Date: 2007-03-27

Last Updated: 2007-03-27

Potential Security Impact: Remote unauthorized arbitrary code execution

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with a Mercury Quality Center ActiveX control. The vulnerability could be exploited by a remote unauthorized user to execute arbitrary code on a Windows client running the ActiveX control.

References: IDEF1930, VU#589097

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
Mercury Quality Center 8.2 Sp1
Mercury Quality Center 9.0

Running on Linux, Solaris, and Windows NT

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

The Hewlett-Packard Company thanks Eric Detoisien and an anonymous researcher working with the iDefense Vulnerability Contributor Program for reporting this vulnerability to security-alert@hp.com

AFFECTED VERSIONS

Action: if Mercury Quality Center is installed, apply the appropriate patch

END AFFECTED VERSIONS

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

Mercury Quality Center 8.2 Sp1 Patch 32:
http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/7a0f7f0efc7905fdc225729f004cf387?OpenDocument

Mercury Quality Center 9.0
Patch 12.1:
http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/cf109e434c7765eac22572a4006c6e94?OpenDocument

PRODUCT SPECIFIC INFORMATION

HISTORY
Version: 1 (rev.1) 27 Mar 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.