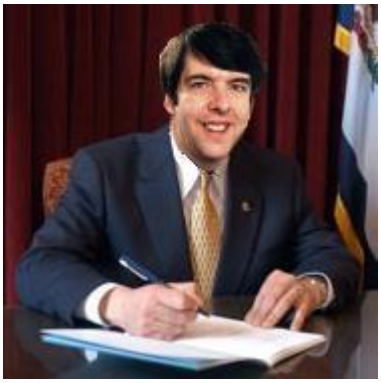
EPING July 2007

This is an archived edition of EPing, first published in July 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 – Green – or Seeing Red?



Our theme for this issue is Linux and there is a lot of Linux-related content elsewhere in E-PING, so I want to stray off subject and talk about data centres.

If you read or watch any media outlet you cannot fail to have noticed in recent weeks that everybody is talking green, and in the IT press, that discussion focuses around the data centre. I've been doing a lot of research into data centres recently, as we're just beginning the process of designing and building a new one on campus.

Some of the facts I've unearthed are enough to make you turn green!

- Data centres account for 1.5% of energy consumption in the UK
- Demand for power in the data centre doubles every five years (Source: Gartner)
- 'Traditional' fully-loaded racks consume between 3 and 10 kWatts. Blade solutions can push this to 30-40 kWatts per rack, and I have heard rumours of one site who are planning for 75 kWatts per rack.
- Traditional air cooling usually cannot cope with more than 10 kWatts per rack; beyond that we need to be looking to water cooling or CO_2 technologies.
- Air conditioning can take as much (or more) power than your IT equipment, although good design can reduce that. (How good a design layout do you have in your machine room?)

However you look at it, we consume a great deal of power. I'm planning for MegaWatts in my new data centre, and a third party hosting service in London has just installed a 13 MegaWatt *upgrade* to their facility.

This power demand therefore has the potential to drive our business into the red - that's assuming of course your energy supplier can deliver the power you need. Many companies' growth is now being stifled by a lack of available power.

With such interest and money around, it's not surprising that HP and others are now offering energy-efficient data centre solutions. Some are radical, involving little less than a complete rebuild of the computer room, but others are more incremental. Design and layout can deliver significant savings. Technology changes in UPS and air conditioning offer promising returns on investment, and the purchase of energy efficient servers will help reduce the power bill. Service and server consolidation and virtualisation will also help reduce your overall inventory, but be warned - Gartner says this will help slow the increase in power demand, but an increase over the years there will still be.

So, pulling us back to our main theme in a contorted way, can Linux consolidation and virtualisation help with your power bills?

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

I look forward to hearing from you.

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

Hints and Tips from Bill Hassell

QUESTION: I have set up a route to our Company's gateway but after a few minutes, the connection is terminated. I am running a newly installed HP-UX 11i system. What is happening?

ANSWER: Try traceroute to the problem machine(s) and see what you find before and after the problem. Another possibility is that for security, your network admin has turned off ICMP echo responses (ping) to the router. The default (for 11.11) is dead gateway detection enabled and opposite to 11.0 defaults.

If you cannot ping the router, after a few minutes, the router (gateway) is deemed to be dead and the route is declared dead. Verify this with:

```
ndd -get /dev/ip ip_ire_gw_probe

ndd -get /dev/ip ip_ire_status
```

If ip_ire_gw_probe is set to 1, then un-pingable routers will be removed from the routing table after a few minutes. Look for the word DEAD in the status report.

To fix it, you'll have to discuss disabling ping responses on the inside of your network with your network-admin. If not negotiable, then you'll have to turn off dead gateway detection in /etc/rc.config.d/nddconf.

If there are no entries, then add:

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_ire_gw_probe
NDD_VALUE[0]=0
```

Then BEFORE you reboot, do this to verify ndd is working for nddconf entries:

```
ndd -get /dev/ip ip_ire_gw_probe
ndd -c
ndd -get /dev/ip ip_ire_gw_probe
```

QUESTION: When I copy files to another directory, the inode usage and the size of the copied directories are different. What is happening?

ANSWER: When you copy files from one filesystem to another you will almost *ALWAYS* have a different amount of space occupied as well as a different number of inodes used. The reasons are twofold: directories and sparse files.

Let's start with directories:

- Directories are just special files that hold information about filenames and inode numbers. When a directory is first created, the size of the directory is 96 bytes. After creating a bunch of files inside the directory, it will grow to accommodate the additional entries. However, if you create 10,000 files in the directory, then remove all but 1 file, the directory will still be several kilobytes in size. The reason is that there are now a bunch of empty slots in the directory but the overhead needed to compress the directory after each file is removed would be enormous, so the directory is left as is with lots of empty slots waiting to be reused. Now if you copy this directory using cp -r or use tar or cpio or any other backup program to

copy the directory to a new location, the directory will be created as 96 bytes and the one file fits nicely in this new directory. But the occupied space shown by du or bdf will be different between the original (which is bigger) and the copy (which is smaller). The result is perfectly OK though.

- Sparse files: This is a file that is created by using lseek to write a new record, then skip a million records and write another record at position 1,000,000. The resultant file contains 2 valid records and 999,998 records full of nulls. On the original system, the space will show up in wc and ls -l but the undefined records are not stored nor counted in bdf or du. Depending on the size of the file and the sparseness, the difference in apparent versus actual size may be VERY large.

Create your own sparse file with:

dd if=/etc/issue of=/var/tmp/sparse bs=4096k seek=1

where you will see the original file is just a few dozen bytes, the result with ls -l or wc -c shows a 4 meg file, but du will show the file as occupying just a bit more than the original /etc/issue file. A cp of the file will create a new file that is the same size (using ls -l or wc -c) but du will now show a MUCH larger size than the original file and it will use more inodes. However, both the original and the copy will diff exactly the same and programs cannot tell any difference between the two files.

So in summary, you can't use bdf or du (or df) to verify a directory copy. Instead, use find to count the files and the directories and if necessary, use ls -l to find the size of both source and destination files and compare those numbers.

QUESTION: How do I control vim to display colors? I'm using vim with the PuTTY terminal emulator and all I see are a few shades of grey.

ANSWER: When is a terminal not a terminal? When it is an emulator. A 'real' terminal has no colors at all, just black and white, or perhaps black and green. You are actually on a PC running a program that takes the PC keyboard and display to 'emulate' a terminal. You'll need to identify exactly what terminal putty is trying to emulate and see whether the ttytype -s command identifies it correctly. This is a combination of terminal emulation (can the putty program display any colors at all?), and if so, can putty be configured to handle different terminfo parameters with different colors (ie, bold=blue, dim=yellow, etc), and if so, change the map in putty. vim (as far as I know) is using the Curses library (and hopefully does not have hardcoded escape sequences internally). For instance, try this little snippet to show the different character enhancements:

```
eval $(ttytype -s)
echo "ttytype says this is a $TERM"
HB=$(/usr/bin/tput dim) # dim text
HV=$(/usr/bin/tput smso) # 1/2 bright inverse IV=$(/usr/bin/tput bold) # inverse
UL=$(/usr/bin/tput smul) # underline BL=$(/usr/bin/tput blink) # blink echo "Normal $IV
Inverse $HB Dim $BL Blink $HV halfbrite $UL underline"
```

This should produce a different enhancement for each feature (there are others in terminfo). If a feature is not present in the terminfo database for this TERM value, tput will return a null string and a non-zero return code. The problem with terminals (and emulators like putty) is that there are so many of them. The good news is that hundreds (about 1800 different models) are included in /usr/lib/terminfo/* so dig out the putty manual to see how video enhancements and colors are handled. The terminfo man page gives some good info about colors too. Look for: Color Manipulation in the man page.

QUESTION: I need to quickly summarize active space on my systems. bdf can do this but it is slow and I really need just the lvol space as well as unassigned space in the volume groups.

ANSWER: Here is a simple script that finds all the volume groups and reports the needed info.

NOTE: It assumes that all volume groups start with /dev/vg*. If this is not the case, change the line "for VG in $(ls -d /dev/vg*)" to match your naming convention:

```
#/usr/bin/sh
# Sep 04 Bill Hassell

# Summarize volume groups

for VG in $(ls -d /dev/vg*)
do
  let PESIZE=$(/sbin/vgdisplay $VG \
    | grep "PE Size" \
    | awk '{print $NF}' )

  let FREE=$(/sbin/vgdisplay $VG \
    | grep "Free PE" \
    | awk '{print $NF}' )*$PESIZE

  let PV=$(/sbin/vgdisplay $VG \
    | grep "Act PV" \
    | awk '{print $NF}' )

  TOT=0
  LVNUM=0
  /sbin/vgdisplay -v $VG 2> /dev/null \
    | grep "Current LE"\
    |awk '{print $3}'\
    |while read
  do
    let TOT=$TOT+$REPLY
    let LVNUM=$LVNUM+1
  done

  let MEGS=$TOT*4
  echo "$VG = used $MEGS megs \c"
  echo "in $LVNUM lvols, \c"
  echo "$FREE megs free, $PV PV"
done
```

QUESTION: I need all of my servers to notify me whenever they are shutdown or rebooted. How can I do this?

ANSWER: Here is a start/stop script for reboot email. NOTE: The script will not be run if the system crashes or has a power failure.

```
#!/sbin/sh
# Sep 2004 Bill Hassell

set -u
umask 022
export PATH=/sbin:/usr/sbin:/usr/bin

#       SEND EMAIL AT SHUTDOWN AND REBOOT
#       ================================
#

# Allowed exit values:
#     0 = success; causes "OK" to show up in checklist.
#     1 = failure; causes "FAIL" to show up in checklist.
#     2 = skip; causes "N/A" to show up in the checklist.
#  Use this value if execution of this script is overridden by the use of a control variable, or if
this script is not appropriate to execute for some other reason.
#     3 = reboot; causes the system to be rebooted after execution.
#     4 = background; causes "BG" to show up in the checklist.
#  Use this value if this script starts a process in background mode.

# Input and output:
#
#    stdin is redirected from /dev/null
#
#    stdout and stderr are redirected to the /etc/rc.log file
#    during checklist mode, or to the console in raw mode.

RETURNVALUE=0
MYHOST=$(hostname)
MYNAME=${0##*/}

# Check the exit value of a command run by this script.
# If non-zero, the exit code is echoed to the rc.log file and # the return value of this script is
set to indicate failure.
# NOTE: do not use EXITCODE as a RETURNVALUE as the start/stop facililty expects the
above exit codes (0,1,2,3)

# Call this function to test the success of an action

set_return()
{
  EXITCODE=$?
  if [ $EXITCODE -ne 0 ]
  then
    echo "Exit code: $EXITCODE"
    RETURNVALUE=1                  # script FAILed
  fi
}

# In case this script is started without any values, assign a #  default

PARM1=${1:-notset}
case $PARM1 in
'start_msg')
```

```
        echo "Sending an email about reboot"
        ;;

'stop_msg')
        echo "Sending an email about shutdown"
        ;;

'start')

      # source the system configuration variables
      if [ -f /etc/rc.config ]
      then
        . /etc/rc.config
      else
        echo "ERROR: /etc/rc.config defaults file MISSING"
      fi

      # Check to see if this script is to start anything...
      #   The default (if $STARTEMAIL is unset) = 0

      STARTEMAIL=${STARTEMAIL:-0}
      if [ "$STARTEMAIL" = 0 ]
      then
        RETURNVALUE=2
      else

      # Send an bootup notice
        mailx -s \
        "$MYHOST rebooted $(date '+%a %b %d %I:%M%p')" \
        $STARTSTOPADDR << EOD
$MYHOST rebooted at $(date)
Last 5 reboots:
$(head -5 /etc/shutdownlog)
EOD
        set_return
      fi
      ;;

'stop')

# source the system configuration variables
      if [ -f /etc/rc.config ]
      then
        . /etc/rc.config
      else
        echo "ERROR: /etc/rc.config defaults file MISSING"
      fi

# Check to see if this script is allowed to stop anything...
# Adjust the code accordingly, HP-UX default has always been
#    to return N/A (RETURNVALUE=2) if the STOPEMAIL = 0

      STOPEMAIL=${STOPEMAIL:-0}
      if [ "$STOPEMAIL" = 0 ]
      then
```

```
        RETURNVALUE=2
      else

# Execute the commands to stop your subsystem (replace :)
        mailx -s \
        "$MYHOST shutdown at $(date '+%a %b %d %I:%M%p')" \
        $STARTSTOPADDR << EOD
$MYHOST rebooted at $(date)
Last 5 reboots:
$(head -5 /etc/shutdownlog)
EOD
        set_return
      fi
      ;;

*)
# All other values are invalid

      echo "usage: $MYNAME {start|stop|start_msg|stop_msg}"
      RETURNVALUE=1
      ;;
esac

exit $RETURNVALUE
```

Like all start/stop scripts, rebootemail must be stored in /sbin/init.d and then sequenced using an symlink in /sbin/rc*.d to be run in the proper order. Here are suggested links:

```
  ln -s /sbin/init.s/rebootemail /sbin/rc2.d/S775rebootemail
  ln -s /sbin/init.s/rebootemail /sbin/rc1.d/K155rebootemail
```

(the choices for S775 and K155 are to sort the order for start and stop. Since this is an email script, make sure the S number follows sendmail start and that the K number is near the front of the list, long before sendmail is shutdown)

And here is the configuration script for /etc/rc.config.d/rebootemail:

```
# enable email to be sent at shutdown and reboot export STARTEMAIL=1 export
STOPEMAIL=1 export STARTSTOPADDR="root@mycpu.com,1234@mypager.net"
```

Edit the above as needed for your email requirements.

Announcing V10 of the OpenVMS Technical Journal

Announcing the latest OpenVMS Technical Journal. Yes folks, V10 is now available in both HTML and PDF.

The OpenVMS Technical Journal is a volunteer technical journal by and for the OpenVMS Community. This version is done with a huge amount of help from Merle Roesler and Warren Sander, not to mention our outstanding authors.

We have six articles in this version:

- Strategies for migrating from Alpha and VAX Systems to HP Integrity Server Systems on OpenVMS
- OpenVMS: Striving to provide the support you need
- Java and OpenVMS:
- Myths and realities
- Implementation of a web application maintenance and testing environment
- Simplification thru Symbols

Please visit the web site at http://h71000.www7.hp.com/openvms/journal/index.html

Warm Regards
Sue Skonetski
OpenVMS Technical Journal Editor

Quantifying the Total Cost for Entry Level and Mid Range Server Clusters

There is a new white paper on Quantifying the Total Cost for Entry Level and Mid Range Server Clusters (a detailed analysis of the total cost of ownership of HP OpenVMS, IBM AIX and SUN Solaris server clusters).

This is one of those white papers that I really encourage you to print a copy of and give to your manager.

Go to: http://h71028.www7.hp.com/ERC/downloads/TechWise_TCO2007.pdf

Warm Regards,
Sue Skonetski, HP

SarCheck® 6.2 FOR HP-UX

APTITUNE CORPORATION ANNOUNCES SarCheck® 6.2 FOR HP-UX

PLAISTOW, NH (June 29, 2007) Aptitune Corporation has announced the general release of SarCheck® Version 6.2 for HP-UX.

SarCheck is a performance management tool designed to assist system administrators in the analysis of system performance by translating the output of several monitoring utilities into a plain English or HTML-formatted report. SarCheck identifies performance bottlenecks, finds runaway processes and memory leaks, recommends changes to various tunable parameters and hardware configurations, and quantifies remaining system capacity.

The most important new features in SarCheck Version 6.2 are the analysis of data from the swapinfo utility, and a complete rewrite of the analysis of both memory pressure and dynamic buffer cache statistics. A variety of other incremental changes have been made to improve the clarity of SarCheck's output and to make the meaning of graphed data more intuitive.

SarCheck is designed to help Systems Administrators learn more about how their systems work by explaining resource utilization and capacity limits in plain English. It uses tools available within the operating system, primarily sar and ps, to learn how the system's resources are being utilized. It then makes recommendations for kernel tuning and hardware upgrades, based on the system's resource utilization. SarCheck also helps the administrator to diagnose problems remotely, and to quickly recommend or implement corrective actions.

Because SarCheck has been specifically designed with safety in mind, it will make detailed recommendations instead of attempting to fix problems itself. It will also explain the reasons for its recommendations.

More information and examples of reports are available at http://www.sarcheck.com

Rick Zecchini, Aptitune Corporation, P.O. Box 1033, Plaistow, NH 03865
Tel.: + 1-603-382-4200
E-mail: sales@sarcheck.com

HP iLO 2 Requirements Survey

The HP iLO team is beginning the process of defining requirements for 2008 releases of iLO 2 firmware. To feedback your requirements, please go to:
http://www.zoomerang.com/survey.zgi?p=WEB226HEESAD99

Useful Linux Links and the ProLiant Support Matrix

Useful Linux Links

General Linux Information from HP www.hp.com/go/linux
Linux Integrity - www.hp.com/go/integritylinux
Linux Workstations - www.hp.com/go/workstationlinux
Linux Desktops - www.hp.com/go/clientlinux
ProLiant Linux - www.hp.com/go/proliantlinux
Red Hat - www.hp.com/go/proliantrhel
SLES - www.hp.com/go/proliantsles
Debian - www.hp.com/go/debian
OEL - www.hp.com/go/oel
Red Flag - www.hp.com/redflag

Proliant Support Matrix

We are trying to encourage customers to reference the certification matrix, which is accessible from the Proliant Linux link:

http://h18004.www1.hp.com/products/servers/linux/hpLinuxcert.html

Recently, IDC reported that HP extended its leadership with Linux in both server units and server revenue. The large majority of this success can be attributed to Linux on HP ProLiant servers. In order for HP to continue and extend this leadership, it's key we understand the customer experience with deploying and using Linux on HP ProLiant servers.

http://www.zoomerang.com/survey.zgi?p=WEB226LQE5B3VL

The survey specifically asks questions on preferred Linux deployment methods and attempts to gather data on usage of HP ProLiant value add software such as Linux ProLiant support packs and version control.

with thanks to Terry Young and Ian Dent, HP

OpenVMS - Do Your Tapes Take Forever to Seek?

Most modern tape drives have the ability to wind onto the EOB (End Of Backup) marker very quickly, but VMS users must explicitly switch this on.

For large capacity LTO/SDLT tapes, this spooling process can take as much as 30 minutes, depending on how much data is on the tape. With 'fastskip' switched on, this becomes a few minutes.

So, if you suffer from this problem on OpenVMS then check your drive supports 'fastskip', and action this command (on all nodes) and watch that tape spin:-

$ SET MAGTAPE /FAST_SKIP=ALWAYS device:

Issuing a '$ SHOW DEV device: /FULL' should show something like this:-

Magtape 2MGA1: (ALPHA), device type HP Ultrium 3-SCSI, is online, record-oriented device, file-oriented device, served to cluster via TMSCP Server, error logging is enabled, controller supports compaction (compaction enabled), device supports fastskip (always).

With thanks to Robert Atkinson

The Quorum Server for Serviceguard

The Quorum Server provides a “tie-breaking” service. Functionally, it behaves in the same way as the “Cluster Lock” behaved when cluster locks were used within an LVM volume group.

This tie-breaking service, either through a Quorum Server or through LVM disks, is needed when the failure of one or more nodes in a cluster results in the surviving cluster nodes trying to reform the cluster. In general, the Quorum Server or LVM cluster lock disk is used as a tiebreaker only for situations in which one or more nodes in the running cluster fails and the resulting cluster is split into two subclusters of equal size. This could happen, for example, when a 2-node cluster loses complete network connectivity.

In this case, each node thinks the other node has died. This condition is sometime referred to as the “split brain syndrome.” In this situation, each node, attempts to reform the cluster as a single-node cluster. Since the two nodes cannot be allowed to reform as single-node clusters in the same subnet and using the same cluster name and the same shared disks, the subcluster that gets the Quorum Server or cluster lock will form the new cluster. The subcluster that does not get the Quorum Server or the cluster lock will panic in order to allow existing applications to failover to the new cluster.

For the full article, please go to:

www.hpug.org.uk/files/serviceguard.pdf

with thanks to Fiona Monteath, HP Education

HP Open Source

HP does a lot more than talk about open source - we're a solutions provider, active user, and a longstanding supporter of the community that drives it. Today, more than 2,500 developers across the company are focused on Linux and open source projects. Over 6,500 service professionals worldwide are involved in the implementation and support of Linux and open source projects. And HP has over 200 shipping products with embedded open source software.

Our track record is a clear indication that we are seriously committed to the growth, maturity, and success of open source technology for our customers, and that fuelling the community with this is mind is an integral part of that effort.

HP supports Linux Foundation

As another example of HP's support of the open source community, HP is a founding platinum member of the new OSDL and FSG merged organization that is determined to help promote, protect, and standardize Linux.

Organisational Leadership

HP has been an active sponsor of numerous open source and Linux organizations towards the stewardship and success of open source technology and its vast user community. Organizations such as the Free Software Foundation, Open Source Software Institute and Linux Foundation are all supported by HP.

For the full article please go to: www.hpug.org.uk/files/OpenSource.pdf

Announcement - OpenVMS on Blades

See the following URL for a letter from Ann McQuaid (HP):
http://h71000.www7.hp.com/news/annmcquaid.pdf
For a direct link to the Blades announcement please visit the HP OpenVMS page:
www.hp.com/go/openvms

with thanks to Sue Skonetski (HP)

More Hints and Tips

HP-UX: Sendmail vs. OpenSource versions cause concern for security auditors

PROBLEM

It is not unusual for security auditors to recommend updating to a more recent version of Sendmail after looking at the version running on a machine.

This can cause concern when the more recent versions of OpenSource sendmail have not been ported to HP-UX, particularly on older HP-UX OS platforms.

CONFIGURATION

Operating System - HP-UX
Version - 11.x
Subsystem - Sendmail 8.9.3, 8.11.1, 8.13.3 and later

RESOLUTION

HP's sendmail v.vv.v is not the same as the OpenSource code with the same revision number. The sendmail version number on HP's sendmail indicates the Open Source base version which was used when the code was ported to HP-UX.

When a significant defect is reported against the sendmail product, the repair is usually addressed in the OpenSource code by releasing a new revision of the latest code. However, HP instead plans to identify and fix significant defects in all supported versions via a patch or new webupgrade. Versions of sendmail which are distributed with the Operating System are patched; versions which are distributed via a webupgrade are updated via a revised webupgrade.

For example, the latest webupgrade sendmail 8.11.1 for HP-UX 11.00 (at the time of writing) is version 5 (B.11.00.01.005).

In case of uncertainty, there are two steps available to confirm whether or not the running version of sendmail contains all required defect repairs:

1. Review the list of defects addressed in the patch or webupgrade version.

Patch documentation lists all defect repairs contained both in the patch itself, and in any patches superseded/replaced by it.

Web upgrades incorporate their own release notes, which are also available on docs.hp.com. For example, sendmail 8.11.1:

http://www.docs.hp.com/en/5990-6693/ch04s03.html#bgecdijd

Additionally, any CERT security bulletins which are applicable to HP-UX should cross-reference the versions of HP-UX sendmail in which the fix is available.

2. Ask security advisors to live test the running version of sendmail using their choice of 3rd party scanning software. (Note that this test should go beyond simply checking the version string returned by the product.)

TechConfSys in HP-UX 11i Version 1.6 MTOE and TCOE

QUESTION

What is the TechSysConf bundle that is introduced as part of the HP-UX 11i Version 1.6 Minimal Technical Operating Environment (MTOE) and the Technical Computing Operating Environment (TCOE)?

ANSWER

TechSysConf addresses needs of HP workstation and technical server customers. The bundle consists of the TC-SysSetup and TC-OpenSource products. These are:
- The TC-SysSetup product alters kernel-configurable parameters, assigning values that are

proven to increase performance in technical environments.
- The TC-OpenSource product delivers a set of high-demand open source software tools, such as emacs and tcsh.

For a complete list of new TechSysConf kernel parameters and values, and a list of the Open Source software tools, refer to the HP-UX 11i Version 1.6 Release Notes at:

http://www.docs.hp.com/

Click on the "Browse by Release" link, then select "HP-UX 11i Version 1.6 Release".
CONFIGURATION

HP-UX 11i Version 1.6

Opensource "scponly" utility to ssh?

PROBLEM

This is an Enhancement Request to add the Opensource "scponly" utility to our ssh product. This product has a very interesting feature which allows some accounts to transfer files only, without allowing login. In security environments, this can be very useful.

Information about it can be found at http://www.sublimation.org/scponly

We have looked at the opensource version of scponly and it does have some bugs that can make the session hang (any commands other than scp). We tried this on Linux as well as we found the same behavior so this is probably part of the design.

We may consider this for Internet Express in the future.

Is Ignite-UX available for Linux?

PROBLEM

Is Ignite-UX available for Linux?

RESOLUTION

Ignite is not available for Linux as it relies heavily on SDUX. Below are links to several opensource projects (GPL) that provide similar functionality:

Mondo Rescue -

http://linux.freak.school.nz/mondo/download.html

Backburner -

http://www.linux.org/apps/AppId_269.html

Port scanning software breaks Data Protector

PROBLEM

Data Protector is failing when Port Scanning Software is enabled. The application is called NMAP. It is an Opensource port scanner. It is used to map the network and classify all active devices.

Configured to simply perform a TCP SYN scan (sends SYN packet to port, when SYN/ACK is received, responds with RST to close connection).

Below are some of the errors seen within the session report:

[81:78] D:\..
Cannot read 20 bytes at offset -20(:2): ([32] The process cannot access the file because it is being used by another process)

[Major] From: VBDA@<hostname> [/D]" Time: 07/24/04 08:13:50 [81:78] D:\
Cannot read 20 bytes at offset -20(:2): ([32] The process cannot access the file because it is being used by another process)

[Major] From: VBDA@<hostname> [/D]" Time: 07/24/04 08:13:50 [81:78] D:\
Cannot read 20 bytes at offset -20(:2): ([32] The process cannot access the file because it is being used by another process).

HP-UX - configuring STARTTLS for sendmail communication with servers that require TLS

PROBLEM

How is STARTTLS configured for communication both with servers requiring Transport Layer Security (TLS) and those which do not?

CONFIGURATION

Operating System - HP-UX
Version - 11.11 and later
Subsystem - Sendmail 8.13.3 with STARTTLS

RESOLUTION

Note that STARTTLS is a feature/functionality provided with HP's port of sendmail 8.13.3 from the Opensource version. However, customers are responsible for understanding and implementing it to meet their own diverse requirements.

Craig Hunt in his "Sendmail Cookbook" (Published by O'Reilly, 1st edition, ISBN 0-596-00471-0) explains the concepts particularly well.

TLS is based on "Asymmetric Encryption" (more commonly called "Public Key Encryption"). It uses two different keys:

- public key

This key is available "to the world". Anyone can access and use it.

- private key

This key belongs to the owner of pair and is a private key that is kept secret.

The keys work together. Anything encrypted with the public key can only be decrypted with the private key, and anything encrypted with the private key can only be decrypted with the public key.

Both the TLS client (the initiator of an SMTP connection) and server (the mailserver receiving the inbound SMTP connection) should have their own public/private key pair, so four keys are needed to authenticate both sides.

A public key is distributed using a file called a "certificate". This file contains a public key which is certified to be valid by a "digital signature" which is also contained in the file.

Digital signatures can be obtained in several ways depending on how the key pair is to be used and the level of trust placed in the signer of the certificate.

1. There are several commercial Certificate Authorities (CAs). For a fee, a commercial CA will sign your "Certificate Request" creating a signed certificate. For a certificate to be accepted worldwide (Internet-wide!) then it is necessary to use a commercial CA to sign the certificate. Commercial CAs are trusted to provide reasonable assurance that the certificate is correct and represents the organization it claims to represent.

2. For communication between sites on an Internal Intranet, or between two parties who have agreed to trust one another, an alternative to using a commercial CA is to create a Private CA. An advantage is that there is no need to involve another organization in order to sign your certificates, but this is also a more complex process than asking a CA to sign your public key certificate.

3. It is also possible to create a "self-signed certificate" which is not signed by any type of CA. This has no element of validation - it is similar to someone printing their own passport! Sendmail does not accept self-signed certificates for authentication because there is no way to verify the content.

Sendmail does, however, accept self-signed certificates for encryption.

With sendmail, TLS can be used for these different purposes:

a. Authentication

b. Encryption (between servers, not end-end)
c. Integrity assurance

First, it is necessary to establish precisely what you want from STARTTLS:

o encryption which only works on a per-hop basis, not end-end
o authentication (the email is genuinely from the sender)
o integrity assurance (the email has not been tampered with)

Sendmail control of STARTTLS is achieved mainly through the access database; therefore, depending on the goal, some configuration may be necessary. Here are some of the steps that need to occur:

1. Install OpenSSL. (Download OpenSSl from http://software.hp.com)

2. Get sendmail.cf built with the correct options, for example:

```
# cd /usr/newconfig/etc/mail/cf/cf
# ./gen_cf
4: Security Options
2: STARTTLS
3: Anti-spamming Options
1: Access DB
  << back to main menu >>
5: Generate sendmail.cf
```

(The above assumes that only the MTA uses STARTTLS, not the MSP.)

3. Copy ./sendmail.cf.gen to /etc/mail/sendmail.cf

4. Update /etc/mail/sendmail.cf to enable STARTTLS - uncomment this option:

```
O UseTLS=True
```

5. This step may be needed if the system has a /dev/random and /dev/urandom devices. If so, then uncomment the following line (or ensure that it is included) in the /etc/mail/sendmail.cf file:

```
O RandFile=egd:/dev/random
```

Once these steps are completed, it is time to configure the certificates. The sendmail.cf file will have several new variables added, all commented. The first of these, UseTLS, was uncommented in step #3 above. The rest of the variables are:

1. CACertPath

CACertPath points to the path of the directory in which the Certificate Authority certificates are held. This can be the same directory as where the client's and server's own certificates are stored too. A typical value for this would be /etc/mail/certs.

2. CACertFile

CACertFile should point to the file (fully qualified path!!) containing the certificate of the root certificate authority. This is going to be the certificate of the CA who signed your certificate. That is, it is a certificate that comes from somewhere and is not self-signed! A typical name would be the /etc/mail/certs/cacert.pem file.

3. ServerCertFile

ServerCertFile should point to the (fully qualified path again!) filename containing the signed certificate which the mailserver will use when it is going to be in the role of a STARTTLS server (in other words, for inbound connections). A typical name would be the /etc/mail/certs/cert.pem file.

4. ServerKeyFile

ServerKeyFile points to the filename containing the private key to be used when the mailserver is in the role of STARTTLS server. A typical name would be the /etc/mail/certs/key.pem file.

5. ClientCertFile

Same as ServerCertFile, only for the client. This can be the same certificate or a different one. Most examples use the same certificate for both.

6. ClientKeyFile

Again, this is the same as ServerKeyFile except it is for the client.

Finally, look at how STARTTLS is enforced (or not). Accessdb is used with STARTTLS to control its use, not to enable or disable the functionality. By default, if this was enabled from gen_cf, if OPENSSL was installed correctly, and if the variables in sendmail.cf point to good key and certificate files, then:

o If STARTTLS is offered by a remote server, then sendmail will try to use it.

o If STARTTLS is not offered by a remote server, then sendmail will not try to use it.

o The sendmail server will offer STARTTLS but will not enforce its use on all inbound connections.

There are special entries in accessdb which control the default requirements for accessdb (if nothing, then optional as explained just now). They are:

o TLS_Serv

This controls the required connection behavior when sendmail makes the outbound connection to another mailserver.

o TLS_Clt

This controls the required connection when the sendmail server receives a connection from

a mail client or another mailserver.

o TLS_Rcpt

This controls the required behavior depending on the mail message recipient.

Each of these entries can be specified on its own to configure the default behavior for all hosts not otherwise declared explicitly, or with a hostname, e.g.:

TLS_Srv:myremoteserv.domain.com

For more details see Sendmail 3rd Edition by Bryan Costales with Eric Allman, published by O'Reilly - ISBN 1-56592-839-3 - starting with section 10.10.8.2 on page 423.

How to compile a module for the HP-UX Apache Web Server

PROBLEM

Please see below for information about how to compile a module to use with the HP-UX Apache Web Server.

CONFIGURATION

Operating System - HP-UX
Version - 11.x
Subsystem - Apache Web Server

RESOLUTION

While HP does ship some PHP extensions, such as

o oci8 (for Oracle),

o GD (related to online creation of graphics), and

o domxml (Document Object Markup with XML),

not all PHP extensions for the HP Apache Web Server are available from HP. However, the extensions themselves can be compiled as illustrated below.

To compile your own PHP extension, a recent version of the HP Apache Web Server is required. HP makes no guarantees, but the following sequence of steps has been known to work successfully.

Building PHP extensions:

Building a custom PHP extension and using it with the HP Apache Web Server may or may not work and is not officially supported, as of the date of this writing, because HP Apache's code base is not identical to the opensource versions due to enhancements and additional

fixes made by HP to improve product quality.

The following information is provided with NO guarantees.

The following steps are typical guidelines for compiling an arbitrary extension. Some extensions may present unique situations that will need to be fixed, but the following steps should apply to PHP 4.x extensions.

1. Download Sources:

In order to build PHP extensions, it is necessary to download the PHP sources from http://www.php.net. Make sure to pick the sources for the same version as the PHP that is part of your HP Apache distribution.

2. Build PHP (optional):

PHP will most likely need to be built in order to generate some of the files required for building the extensions. However, the next step (#3) might work without performing this step. If this step is skipped, and step 3 fails, then simply perform this step and try #3 again.

3. Prepare the extension sources for running configure:

"autoconf" and "aclocal" are needed for this step:

a. "cd" to the directory of the extension you want to build.

b. Run /$pathToPhpSource/scripts/phpize.

4. Run Configure to generate Makefile:

For example:

```
/configure --prefix=/opt/hpws/apache/php \
        --with-php-config= /$pathToPhpSource/scripts/php-config
        --other-extension-specific-options
```

Any "$pathToPhpSource/scripts" can also be substituted with "/opt/hpws/apache/php/bin". (This is the preferred method if it works.)

5. Perform fix-ups prior to make:

Edit libtool and change the value of deplibs_check_method as follows

deplibs_check_method=pass_all

6. Run make:

At the end of the following two steps, a binary should be available for the extension:

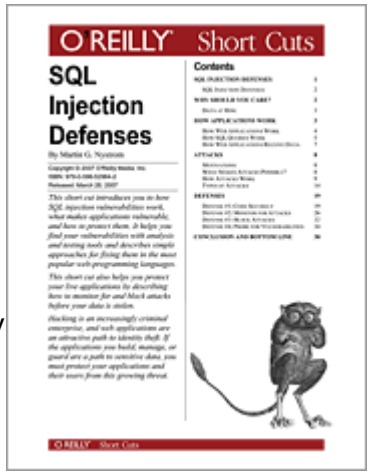
a. make

b. make install

Once the binary is created, add the new extension into the php.ini file and restart the Apache web server.

Book Review – SQL Injection Defenses

Martin Nystrom brings us his insight into why hackers attempt to get into our databases and what we should do to keep them out. This O'Reilly "Short Cut" is certainly not the definitive volume on defending your applications, and isn't designed to be, but will give you the understanding required to go further into making your systems secure.



The narrative is split into 3 main sections –

- A basic overview of the technologies involved, and why someone would want to exploit your systems
- What the attacks look like and how they're performed
- A number of methods showing how you can defend your systems against attack

The author expects his reader to have some understanding of the programming languages used in the article, namely Perl, PHP, VB.Net and Java. From there he takes us through a variety of examples, showing how bad code allows the hacker in, and the tools within the various languages that help us keep them out.

He also emphasises the other non-coding methods we can use to stop or at least detect attacks, such as Cisco's AVS system. According to his own narrative, these are difficult and time consuming to set up, but worth it for specific high-profile applications.

One of the interesting comments made is that the 'Information Security' magazine systems were broken into. It leaves you asking what's the point if they can't defend themselves? Of course, almost every system is vulnerable in some way, but our task is to reduce that risk down as much as feasibly possible, and Martin does help us achieve that.

An area the book particularly highlights is PHP vulnerabilities, showing that it's ease design and speed of deployment is also it's Achilles Heal. However, there are also 'built in' ways that even PHP can defend itself against the most hardened attacker.

The text is interlaced with screen shots of various applications at work, but in some ways, this is it's down side. After reading the book through a few times, I felt I'd been educated and would be able to take what I'd learnt into a real situation. What Martin could have done is drop some of the images not relevant to the subject matter and some of the repetitive description, and replaced it with some more 'Meat on the bones'.

As the book is delivered in a PDF version it makes it worth having around as a reminder of what can happen if you don't educate your developers in the right techniques. Some of the examples shown will certainly shock the novice programmer, showing just how easily your data can be compromised.

More information can be found on the O'Reilly site at
http://www.oreilly.com/catalog/9780596529642/index.html

HP Security Bulletins – HP-UX

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01067768

Version: 1

HPSBUX02218 SSRT071424 rev.1 - HP-UX running CIFS Server (Samba), Remote Arbitrary Code Execution

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

Release Date: 2007-05-29

Last Updated: 2007-06-04

Potential Security Impact: Remote arbitrary code execution

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

VULNERABILITY SUMMARY
Potential vulnerabilities have been identified with HP-UX running CIFS Server (Samba). The vulnerabilities could be exploited remotely to execute arbitrary code.

References: CVE-2007-2446, CVE-2007-2447

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.11.31 running CIFS Server (Samba) A.02.01, A.02.01.01,A.02.01.02, A.02.02, A.02.02.01, A.02.02.02, A.02.03, A.02.03.01.

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 an affected fileset. Then determine if the recommended patch or update is installed.

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
HP-UX B.11.31
==========
CIFS-Server.CIFS-ADMIN
CIFS-Server.CIFS-DOC
CIFS-Server.CIFS-LIB
CIFS-Server.CIFS-MAN
CIFS-Server.CIFS-RUN
CIFS-Server.CIFS-UTIL
action: install revision A.02.03.02 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following available to resolve the vulnerability:

HP-UX release CIFS Server (Samba) revision Install recommendation B.11.11, B.11.23, B.11.31 A.02.01, A.02.01.01, A.02.01.02, A.02.02, A.02.02.01, A.02.02.02, A.02.03, A.02.03.01 revision A.02.03.02 or subsequent

The updates can be downloaded from http://www.hp.com/go/softwaredepot/

MANUAL ACTIONS: Yes - Update

CIFS / Samba on HP-UX B.11.11 install revision A.02.03.02 or subsequent.

CIFS / Samba on HP-UX B.11.23 install revision A.02.03.02 or subsequent.

CIFS / Samba on HP-UX B.11.31 install revision A.02.03.02 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) - 04 June 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: c01056923

Version: 2

HPSBUX02217 SSRT071337 rev.2 - HP-UX running Kerberos, Remote Arbitrary Code Execution

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

Release Date: 2007-05-15

Last Updated: 2007-05-25

Potential Security Impact: Remote arbitrary code execution

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified on HP-UX running Kerberos. The vulnerability could be exploited by remote authorized users to execute arbitrary code.

References: CVE-2007-1216

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, and B.11.31 running the Kerberos Client software versions 1.3.5.05 and previous.

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

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

AFFECTED VERSIONS

HP-UX B.11.11
==========
krb5client.KRB5-64SLIB-A
krb5client.KRB5-E-A-MAN-A
krb5client.KRB5-J-E-MAN-A
krb5client.KRB5-J-S-MAN-A
krb5client.KRB5-PRG-A
krb5client.KRB5-RUN-A
krb5client.KRB5-SHLIB-A
action: install revision C.1.3.5.06 or subsequent

KRB5-Client.KRB5-SHLIB
KRB5-Client.KRB5-PRG
KRB5-Client.KRB5-RUN
KRB5-Client.KRB5-ENG-A-MAN
KRB5-Client.KRB5-JPN-E-MAN
KRB5-Client.KRB5-JPN-S-MAN
KRB5-Client.KRB5-64SLIB
action: install PHSS_36286 or subsequent

HP-UX B.11.23
==========
krb5client.KRB5-64SLIB-A
krb5client.KRB5-E-A-MAN-A
krb5client.KRB5-J-E-MAN-A
krb5client.KRB5-J-S-MAN-A
krb5client.KRB5-PRG-A
krb5client.KRB5-RUN-A
krb5client.KRB5-SHLIB-A
krb5client.KRB5IA32SLIB-A
krb5client.KRB5IA64SLIB-A
action: install revision D.1.3.5.06 or subsequent

KRB5-Client.KRB5-64SLIB
KRB5-Client.KRB5-ENG-A-MAN
KRB5-Client.KRB5-IA32SLIB
KRB5-Client.KRB5-IA64SLIB
KRB5-Client.KRB5-JPN-E-MAN
KRB5-Client.KRB5-JPN-S-MAN
KRB5-Client.KRB5-PRG
KRB5-Client.KRB5-RUN

KRB5-Client.KRB5-SHLIB
action: install PHSS_34991 or subsequent

HP-UX B.11.31
==========
KRB5-Client.KRB5-64SLIB
KRB5-Client.KRB5-IA32SLIB
KRB5-Client.KRB5-IA64SLIB
KRB5-Client.KRB5-SHLIB
KRB5-Client.KRB5-64SLIB
KRB5-Client.KRB5-SHLIB
action: install PHSS_36361 or subsequent

END AFFECTED VERSIONS

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

B.11.11 PHSS_36286 or Kerberos Client C.1.3.5.06 or subsequent
B.11.23 PHSS_34991 or Kerberos Client D.1.3.5.06 or subsequent
B.11.31 PHSS_36361 or subsequent

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

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

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) - 21 May 2007 Initial release
Version: 2 (rev.2) - 29 May 2007 Corrected typo in Reference

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: c01075678

Version: 1

HPSBUX02225 SSRT071295 rev.1 - HP-UX Running Xserver, Local Denial of Service

(DoS)

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

Release Date: 2007-06-12

Last Updated: 2007-06-12

Potential Security Impact: Local Denial of Service (DoS)

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP-UX running Xserver. These vulnerabilities could be exploited by a local user to create a Denial of Service (DoS).

References: CVE-2006-6101, CVE-2006-6102, CVE-2006-6103

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, B.1131 running Xserver

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

AFFECTED VERSIONS

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

HP-UX B.11.11
Xserver.X11-SERV
action: install PHSS_34389 or subsequent

HP-UX B.11.23
Xserver.X11-SERV
Xserver.OEM-SERVER
action: install PHSS_36452 or subsequent

HP-UX B.11.31
Xserver.X11-SERV
Xserver.OEM-SERVER
action: install PHSS_36123 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following patches available to resolve the vulnerabilities. These patches can be downloaded from http://itrc.hp.com/

HP-UX B.11.11 PHSS_34389 or subsequent
HP-UX B.11.23 PHSS_36452 or subsequent
HP-UX B.11.31 PHSS_36123 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) - 12 June 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: c01070495

Version: 1

HPSBUX02219 SSRT061273 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS)

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

Release Date: 2007-06-11

Last Updated: 2007-06-11

Potential Security Impact: Remote Denial of Service (DoS)

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

VULNERABILITY SUMMARY
Potential vulnerabilities have been identified with HP-UX running BIND. The vulnerabilities could be exploited remotely to create a Denial of Service (DoS).

References: CVE-2006-4339, CVE-2007-0493 (BIND v9.3.2 only), CVE-2007-0494

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, and B.11.23 running BIND v9.2.0 or BIND v9.3.2.

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

AFFECTED VERSIONS

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.

For BIND v9.2.0

HP-UX B.11.11
BINDv920.INETSVCS-BIND
action: install revision B.11.11.01.009 or subsequent

HP-UX B.11.23
InternetSrvcs.INETSVCS2-RUN
action: install PHNE_35920 or subsequent

For BIND v9.3.2

HP-UX B.11.11
BindUpgrade.BIND-UPGRADE
action: install revision C.9.3.2.1.0 or subsequent

HP-UX B.11.23
BindUpgrade.BIND-UPGRADE
BindUpgrade.BIND2-UPGRADE
action: install revision C.9.3.2.1.0 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made the following available to resolve the vulnerability:

BIND v9.2.0 HP-UX B.11.11 revision B.11.11.01.009 or subsequent Download information below.

BIND v9.2.0 HP-UX B.11.23 PHNE_35920 or subsequent available from http://itrc.hp.com/

BIND v9.3.2 HP-UX B.11.11 revision C.9.3.2.1.0 or subsequent available from http://www.hp.com/go/softwaredepot

BIND v9.3.2 HP-UX B.11.23 revision C.9.3.2.1.0 or subsequent available from http://www.hp.com/go/softwaredepot

Downloading BIND v9.2.0 revision B.11.11.01.009

For a period of thirty days after the initial release of this Security Bulletin, BIND v9.2.0 revision B.11.11.01.009 will be available for download from the following ftp site. After the ftp site is removed, please contact HP Support to receive this update.

ftp://ss061273:ss061273@hprc.external.hp.com/

The depot is contained in this gzip file: BIND920_v9.depot.gz. It should be unpacked with gunzip(1) and installed with swinstall(1M).

MD5 sum:
MD5 (BIND920_v9.depot) = 23335741e42769502623d863d121cd97

cksum:
1935343678 20766720 BIND920_v9.depot

MANUAL ACTIONS: Yes - Update

BIND v9.2.0 HP-UX B.11.11 install revision B.11.11.01.009 or subsequent.

BIND v9.3.2 HP-UX B.11.11 install revision C.9.3.2.1.0 or subsequent.

BIND v9.3.2 HP-UX B.11.23 install revision C.9.3.2.1.0 or subsequent.

PRODUCT SPECIFIC INFORMATION

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

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

HISTORY
Version: 1 (rev.1) - 11 June 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: c00579189

Version: 5

HPSBUX02087 SSRT4728 rev.5 - HP-UX running TCP/IP Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.
Release Date: 2005-12-09

Last Updated: 2007-05-21

Potential Security Impact: Remote Denial of Service (DoS)

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

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

References: CVE-2004-0744

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.00, B.11.04, B.11.11, B.11.23 running TCP/IP.

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

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

AFFECTED VERSIONS

HP-UX B.11.00
>Streams.STREAMS-KRN
action: install PHNE_30161 or subsequent

HP-UX B.11.04
Networking.NET-KRN
action: install PHNE_33427 or subsequent and install sqmax (see Resolution section)

HP-UX B.11.11
Streams.STREAMS-KRN
action: install PHNE_34131 or subsequent

HP-UX B.11.23
Streams.STREAMS2-KRN
action: install PHKL_31500 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has made patches and product updates available to resolve the issue. After installing the recommended patches for B.11.04 a system parameter must be set. A utility, sqmax, must be downloaded and installed to set the required system parameter as discussed below.

B.11.00 install PHNE_30161 or subsequent sqmax not required
B.11.04 install PHNE_33427 or subsequent then install sqmax as discussed below
B.11.11 install PHNE_34131 or subsequent sqmax not required
B.11.23 install PHKL_31500 or subsequent sqmax not required

The patches are available from http://itrc.hp.com/

For B.11.04:
After the patches listed above are installed an internal system parameter must be set. A utility, sqmax, has been provided to set the parameter.
The sqmax utility is available by writing to security-alert@hp.com

MANUAL ACTIONS: Yes - NonUpdate
B.11.04 - After installing patch, install sqmax. Run "/usr/contrib/bin/sqmax 1000" or reboot.

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) 14 December 2005 Initial release
Version:2 (rev.2) 24 July 2006 New sqmax utility for B.11.04, augmented installation instructions
Version:3 (rev.3) 31 July 2006 PHNE_34131 is available for B.11.11
Version:4 (rev.4) 09 October 2006 PHNE_30161 is available for B.11.00
Version:5 (rev.5) 21 May 2007 Corrected fileset information for PHNE_30161

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: c01091459

Version: 1

HPSBTU02233 SSRT071424 rev.1 - HP Tru64 UNIX Internet Express running Samba, Remote Arbitrary Code Execution or Local Unauthorized Privilege Elevation

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

Release Date: 2007-06-27

Last Updated: 2007-06-27

Potential Security Impact: Remote Arbitrary Code Execution or Local Unauthorized Privilege Elevation

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

VULNERABILITY SUMMARY
Potential vulnerabilities have been identified with Samba provided with HP Internet Express for Tru64 UNIX (IX) v 6.6. The potential vulnerabilities could be exploited by a remote, unauthenticated user to execute arbitrary commands or by a local, unauthorized user to gain privilege elevation.

References: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447

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

HP Internet Express for Tru64 UNIX (IX) v 6.6 running Samba v 3.0.23

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

RESOLUTION
Until the update is available in the mainstream product release, HP is releasing the following setld-based Samba kit publicly for use by any customer.

The resolutions contained in the Samba kit are targeted for availability in the following

mainstream product release:

HP Internet Express for Tru64 UNIX v 6.7

The kit distributes the following:

Samba v 3.0.25
Samba sources and license agreement

HP Internet Express for Tru64 UNIX - Samba 3.0.25
Prerequisite: HP Internet Express for Tru64 UNIX v 6.6
Name: IX66-SAMBA-20070528.tar.gz
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=IX66-SAMBA-20070530

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) - 27 June 2007 Initial release. This is a replacement for Security Bulletin HPSBTU02218 (Document ID: c01078980) that is otherwise identical in order to avoid a possible identification conflict with a different Security Bulletin.

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: c01086137

Version: 1

HPSBTU02232 SSRT071429 rev.1 - Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) or HP Internet Express for Tru64 UNIX running PHP, Remote Arbitrary Code Execution, Unauthorized Disclosure of Information, or Denial of Service (DoS)

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

Release Date: 2007-06-25

Last Updated: 2007-06-25

Potential Security Impact: Remote Arbitrary Code Execution, Unauthorized Disclosure of Information, or Denial of Service (DoS)

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

VULNERABILITY SUMMARY
Potential vulnerabilities have been reported on the PHP Hypertext Processing Engine

provided with the Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) and HP Internet Express for Tru64 UNIX (IX). The vulnerabilities could be exploited by remote users to execute arbitrary code, read arbitrary files, or cause a Denial of Service (DoS).

References: CVE-2006-4625 CVE-2007-0988 CVE-2007-1286 CVE-2007-1380 CVE-2007-1700 CVE-2007-1701 CVE-2007-1710 CVE-2007-1835 CVE-2007-1884 CVE-2007-1885 CVE-2007-1886

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
The following supported software versions running running PHP Hypertext Processing Engine v 4.4.4 are affected:

HP Internet Express for Tru64 UNIX (IX) v 6.6 and earlier Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) v 6.6.4 and earlier

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

RESOLUTION
HP is providing PHP v 4.4.6 as part of Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) v 6.6.5, which resolves the potential vulnerabilities.

Until the update is available in the mainstream product release, HP is releasing the following two setld-based kits publicly for use by any customer.

The resolutions contained in the kits are targeted for availability in the following mainstream product release:

HP Internet Express for Tru64 UNIX v 6.7

The kits distribute the following:

Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) with PHP v 4.4.6 installable kit

Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) with PHP v 4.4.6 installable kit and source files

Secure Web Server for HP Tru64 UNIX v 6.6.5
PREREQUISITE: HP Tru64 UNIX v 5.1A or later
Name: sws_v6_6_5_kit.tar.gz
Location: http://h30097.www3.hp.com/internet/download.htm#sws

Secure Web Server for HP Tru64 UNIX v 6.6.5 including Source Files
PREREQUISITE: HP Tru64 UNIX v 5.1A or later
Name: sws_v6_6_5_src_kit.tar.gz
Location: http://h30097.www3.hp.com/internet/download.htm#sws

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) - 25 June 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: c01078980

Version: 1

HPSBTU02218 SSRT071424 rev.1 - HP Tru64 UNIX Internet Express running Samba, Remote Arbitrary Code Execution or Local Unauthorized Privilege Elevation

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

Release Date: 2007-06-18

Last Updated: 2007-06-18

Potential Security Impact: Remote Arbitrary Code Execution or Local Unauthorized Privilege Elevation

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

VULNERABILITY SUMMARY
Potential vulnerabilities have been identified with Samba provided with HP Internet Express for Tru64 UNIX (IX) v 6.6. The potential vulnerabilities could be exploited by a remote, unauthenticated user to execute arbitrary commands or by a local, unauthorized user to gain privilege elevation.

References: CVE-2007-2444, CVE-2007-2446, CVE-2007-2447

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

HP Internet Express for Tru64 UNIX (IX) v 6.6 running Samba v 3.0.23

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

RESOLUTION
Until the update is available in the mainstream product release, HP is releasing the following setld-based Samba kit publicly for use by any customer.

The resolutions contained in the Samba kit are targeted for availability in the following mainstream product release:

HP Internet Express for Tru64 UNIX v 6.7

The kit distributes the following:

Samba v 3.0.25
Samba sources and license agreement

HP Internet Express for Tru64 UNIX - Samba 3.0.25
Prerequisite: HP Internet Express for Tru64 UNIX v 6.6
Name: IX66-SAMBA-20070528.tar.gz
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=IX66-SAMBA-20070530

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) - 18 June 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: c01007552

Version: 1

HPSBTU02209 SSRT071323 rev.1 - HP Tru64 UNIX Running Secure Shell (SSH), Remote Unauthorized Identification of Valid Users

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, unauthorized identification of valid Users

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP Tru64 UNIX running Secure Shell (SSH). The vulnerability could be exploited remotely by an unauthorized user to identify valid users.

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

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

The Hewlett-Packard Company thanks Andrea Purificato 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

Special Instructions for the Customer:

This patch adds a new keyword to the sshd2_config configuration file for the sshd2 daemon. The new keyword, AuthInteractiveFailureRandomTimeout , adds a random delay to the existing AuthInteractiveFailureTimeout delay. See the sshd2_config man page for information on AuthInteractiveFailureTimeout.

The AuthInteractiveFailureRandomTimeout keyword can take a value from 0 to 100 (in seconds). The default is 2. To disable AuthInteractiveFailureRandomTimeout, specify a value of 0. When a non-zero value is specified for this keyword, a random number of milliseconds up to the number of seconds specified multiplied by 1000 is added to the server delay specified by AuthInteractiveFailureTimeout.

HP Tru64 UNIX Version v5.1B-4
Prerequisite: HP Tru64 UNIX v5.1B-4 PK6 (BL27)
Kit Name: T64KIT1001208-V51BB26-ES-20070427
Kit Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001208-V51BB26-ES-20070427

HP Tru64 UNIX Version v5.1B-3
Prerequisite: HP Tru64 UNIX v5.1B-3 PK5 (BL26)
Kit Name: T64KIT1001205-V51BB27-ES-20070427
Kit Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001205-V51BB27-ES-20070427

MD5 checksums are available from the ITRC patch database main page.

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) - 9 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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00967144

Version: 2

HPSBTU02207 SSRT061239 rev.2 - HP Tru64 UNIX OpenSSL 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: 2007-06-21

Last Updated: 2007-06-21

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 OpenSSL 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 (OpenSSL) VU#697164, VU#915404, CVE-2007-0493, CVE-2007-0494, SSRT061213, SSRT071304 (BIND)

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

HP Tru64 UNIX v 5.1B-4 (OpenSSL and BIND) HP Tru64 UNIX v 5.1B-3 (OpenSSL 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 (OpenSSL)

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

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
Prerequisite: HP Tru64 UNIX v 5.1B-4 PK6 (BL27)
Name: T64KIT1001167-V51BB27-ES-20070321
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001227-V51BB27-ES-20070531

HP Tru64 UNIX Version 5.1B-3
Prerequisite: HP Tru64 UNIX v 5.1B-3 PK5 (BL26)
Name: T64KIT1001163-V51BB26-ES-20070315
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001163-V51BB26-ES-20070315

HP Tru64 UNIX Version 5.1A PK6
Prerequisite: HP Tru64 UNIX v 5.1A PK6 (BL24)
Name: T64KIT1001160-V51AB24-ES-20070314
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001160-V51AB24-ES-20070314

HP Tru64 UNIX Version 4.0G PK4
Prerequisite: HP Tru64 UNIX v 4.0G PK4 (BL22)
Name: T64KIT1001166-V40GB22-ES-20070316
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001166-V40GB22-ES-20070316

HP Tru64 UNIX Version 4.0F PK8
Prerequisite: HP Tru64 UNIX v 4.0F PK8 (BL22)
Name: DUXKIT1001165-V40FB22-ES-20070316
Location: http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1001165-V40FB22-ES-20070316

HP Insight Management Agents for Tru64 UNIX patch version 3.6.1 (for kit CPQIIM360)
Prerequisite: HP Tru64 UNIX v 5.1B-4 PK6 (BL27), v 5.1A PK6 (BL24), v 4.0G PK4 (BL22) or v 4.0F PK8 (BL22)
Name: CPQIM360.SSL.01.tar.gz
Location: http://h30097.www3.hp.com/cma/patches.html

Internet Express (IX) v6.6 BIND
Note: Customers who use Internet Express (IX) v6.6 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
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 v5.1B-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
Version:2 (rev.2) - 21 June 2007 Provides the location of an updated Early Release Patch (ERP) kit for HP Tru64 UNIX v 5.1B-4 (BL27). The updated ERP resolves kit installation problems experienced by some customers. The kits for the other versions listed in this Security Bulletin remain unchanged.

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 – Microsoft/SMA

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01053540

Version: 1

HPSBST02214 SSRT071422 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-023 to MS07-029

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

Release Date: 2007-05-11

Last Updated: 2007-05-15

Potential Security Impact: Please check the table below

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

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

References: MS07-023, MS07-024, MS07-025, MS07-026, MS07-027, MS07-028, MS07-029.

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
MS07-023
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution
(934233) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue
MS07-024

Vulnerabilities in Microsoft Word Could Allow Remote Code Execution
(934232) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue
MS07-025
Vulnerability in Microsoft Office Could Allow Remote Code Execution
(934873) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue
MS07-026
Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution
(931832) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue
MS07-027
Cumulative Security Update for Internet Explorer (931768) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.
Impacts only: Internet Explorer 6 SP1 - or - Internet Explorer 5.01 SP4 To determine your IE version check the IE help page.
MS07-028
Vulnerability in CAPICOM Could Allow Remote Code Execution (931906) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue
MS07-029
Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution
(935966) SMA does not have this component.
Patch will not run successfully. Customers should not be concerned with this issue

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

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

The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:
http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

PRODUCT SPECIFIC INFORMATION

HISTORY

Version: 1 (rev.1) - 15 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 – Storage Management Appliance

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01082087

Version: 1

HPSBST02231 SSRT071438 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-030 to MS07-035

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

Release Date: 2007-06-20

Last Updated: 2007-06-20

Potential Security Impact: Please check the table below

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

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

References: MS07-030, MS07-031, MS07-032, MS07-033, MS07-034, MS07-035.

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

MS07-030
Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (927051) SMA does not have this component.
Patch will not run successfully.
Customers should not be concerned with this issue

MS07-031
Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.

MS07-032
Vulnerability in Windows Vista Could Allow Information Disclosure (931213) SMA does not have this component.
Patch will not run successfully.
Customers should not be concerned with this issue

MS07-033
Cumulative Security Update for Internet Explorer (933566) Possible security issue exists.
Patch will run successfully. For SMA v2.1, customers should download patch from Microsoft and install.
Impacts only: Internet Explorer 6 SP1 - or - Internet Explorer 5.01 SP4
To determine your IE version check the IE help page.

MS07-034
Cumulative Security Update for Outlook Express and Windows Mail (929123) SMA does not have this component.

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

MS07-035
Vulnerability in Win 32 API Could Allow Remote Code Execution (935839) 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

PRODUCT SPECIFIC INFORMATION

HISTORY

Version: 1 (rev.1) - 20 June 2007 Initial release

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

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

HP Security Bulletins – System Management Homepage

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01056506

Version: 1

HPSBMA02215 SSRT071423 rev.1 - HP System Management Homepage (SMH) for Linux and Windows Running PHP, Remote Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.
Release Date: 2007-05-21

Last Updated: 2007-05-21

Potential Security Impact: Remote execution of arbitrary code

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified in PHP, an open source software

component supplied with HP System Management Homepage (SMH). These vulnerabilities could by exploited remotely resulting in the execution of arbitrary code.

References: CVE-2006-4625, CVE-2007-0988, CVE-2007-1286, CVE-2007-1380, CVE-2007-1700, CVE-2007-1701, CVE-2007-1710, CVE-2007-1835, CVE-2007-1884, CVE-2007-1885, CVE-2007-1886

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) versions prior to 2.1.8 running on Linux and Windows.

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

RESOLUTION
HP has provided System Management Homepage (SMH) version 2.1.8 or subsequent for each platform to resolve this issue.

HP System Management Homepage for Linux (x86) version 2.1.8-177 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26864.html

HP System Management Homepage for Linux (AMD64/EM64T) version 2.1.8-177 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26866.html

HP System Management Homepage for Windows version 2.1.8-179 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26977.html

PRODUCT SPECIFIC INFORMATION
HISTORY:
Version:1 (rev.1) - 21 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.

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c01072894

Version: 1

HPSBMA02224 SSRT071334 rev.1 - HP System Management Homepage (SMH) for Linux, Remote Privileged Access

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

Release Date: 2007-06-12

Last Updated: 2007-06-12

Potential Security Impact: Remote privileged access

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP System Management Homepage (SMH) for Linux. This vulnerability could be exploited remotely to gain privileged access.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) versions prior to v2.1.9 running on Linux systems that belong to Novell's e-directory implementation of directory services.

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

With SMH prior to v2.1.9 Novell e-directory members are handled as members of the root group. Therefore, these e-directory members are given privileged access to SMH.

Note: SMH does not support running on the e-directory implementation of directory services.

RESOLUTION
HP has provided the following software updates to resolve the vulnerability:

System Management Homepage (SMH) v2.1.9 or subsequent

HP System Management Homepage for Linux (x86) v2.1.9-178 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/27264.html

HP System Management Homepage for Linux (AMD64/EM64T) v2.1.9-178 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/27263.html

PRODUCT SPECIFIC INFORMATION
HISTORY:
Version:1 (rev.1) - 12 June 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: c01056592

Version: 1

HPSBMA02216 SSRT071310 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Cross Site Scripting (XSS)

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

Release Date: 2007-05-30

Last Updated: 2007-05-30

Potential Security Impact: Remote cross site scripting (XSS)

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP System Management Homepage (SMH) for Linux and Windows. These vulnerabilities could by exploited remotely resulting in cross site scripting (XSS).

References: JVN#19240523

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP System Management Homepage (SMH) versions prior to v2.1.2 running on Linux and Windows.

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

Note: One of the potential vulnerabilities affects older versions of SMH. These older versions are no longer supplied. They can be identified by the following text: "Compaq HTTP Server vX.Y" where X is 5 or lower.

The text is displayed in the bottom left corner of the page displayed at:
http://server:2301/ or https://server:2381/

Customers running these versions of SMH should contact HP Support for upgrade information.

RESOLUTION
HP has provided System Management Homepage (SMH) v2.1.2 or subsequent to resolve these vulnerabilities. The current version, SMH v2.1.8, is available from the following web sites:

HP System Management Homepage for Linux (x86) v2.1.8-177 can be downloaded from
http://h18023.www1.hp.com/support/files/server/us/download/26864.html

HP System Management Homepage for Linux (AMD64/EM64T) v2.1.8-177 can be downloaded from http://h18023.www1.hp.com/support/files/server/us/download/26866.html

HP System Management Homepage for Windows v2.1.8-179 can be downloaded from
http://h18023.www1.hp.com/support/files/server/us/download/26977.html

PRODUCT SPECIFIC INFORMATION

HISTORY:
Version:1 (rev.1) - 30 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.

HP Security Bulletins – Miscellaneous

SUPPORT COMMUNICATION - SECURITY BULLETIN Document ID: c00901872

Version: 3

HPSBGN02199 SSRT071312 rev.3 - 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: 2007-03-13

Last Updated: 2007-06-20

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 Will Dormann of CERT/CC, 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

None

HISTORY
Version:1 (rev.1) - 27 Mar 2007 Initial release
Version:2 (rev.2) - 19 June 2007 Modified acknowledgment to include Will Dormann of CERT/CC
Version:3 (rev.3) - 20 June 2007 Correct version/rev mismatch

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: c01077085

Version: 1

HPSBPI02226 SSRT061274 rev.1 - HP Help and Support Center Running on HP Notebook Computers Running with Windows XP, Remote Unauthorized Access

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

Release Date: 2007-06-18

Last Updated: 2007-06-18

Potential Security Impact: Remote unauthorized access

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified in HP Help and Support Center running on HP Notebook Computers running with Windows XP. The vulnerability could be remotely exploited to allow unauthorized access to the system.

References: CVE-2007-3180

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Help and Support Center earlier than v4.4 C running on HP Notebook Computers running with Microsoft Windows XP, XP Professional, XP Home Edition, XP Tablet PC Edition

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

This issue will only be on HP Notebook Computers that have HP Help and Support with a version less than v4.4 C.

To find the HP Help and Support version using Add/Remove programs:

Click Start
Click Control Panel
Click Add or Remove programs
Scroll to HP Help and Support
Click on the "Click here for support information" link The version number is displayed.
Note: If HP Help and Support is not found in the Add/Remove Programs list, no further action is required.

The Hewlett-Packard Company thanks Karl Lynn of Juniper Networks J-Security Research Labs for reporting this vulnerability to security-alert@hp.com

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

HP Help and Support Center v4.4 C or later

The updated HP Help and Support Center software is available for download at the HP Customer Care site.
Please click on the following link and then select the appropriate language:
http://h10025.www1.hp.com/ewfrf/wc/genericSoftwareDownloadIndex?softwareitem=ob-48738-1&jumpid=reg_R1002_USEN

PRODUCT SPECIFIC INFORMATION

None

HISTORY:
Version:1 (rev.1) - 18 June 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: c01049713

Version: 1

HPSBMA02213 SSRT061214 rev.1 - HP Systems Insight Manager (SIM) for Windows, Remote Privileged Access and Arbitrary Code Execution

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

Release Date: 2007-05-08

Last Updated: 2007-05-14

Potential Security Impact: Remote privileged access or arbitrary code execution

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP Systems Insight Manager (SIM) for Windows. The vulnerability could be exploited to allow remote privileged access and arbitrary code execution.

References: ASPR-2007-05-14-1-PUB

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP SIM 4.2
HP SIM 5.0 SP4
HP SIM 5.0 SP5

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

The Hewlett-Packard Company thanks Luka Treiber and Aljosa Ocepek from Acros Security (www.acrossecurity.com) for reporting this vulnerability to security-alert@hp.com

RESOLUTION
HP has made the following software update available to resolve the vulnerability.
The update is available on:
http://h18013.www1.hp.com/products/servers/management/hpsim/dl_windows.html#windows

HP SIM 5.1 with SP1 - Windows (or subsequent)

PRODUCT SPECIFIC INFORMATION

HISTORY
Version: 1 (rev.1) - 14 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.