

Sec. Vulnerability in SNMP (rev. 1)

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2002-02/0334.html>

From: Security Alert (secure@cup.hp.com)

Date: 02/16/02

From: secure@cup.hp.com (Security Alert)

Date: 16 Feb 2002 16:22:36 GMT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Digest Name: daily HP-UX security bulletins digest

Created: Thu Feb 14 13:00:06 PST 2002

Table of Contents:

Document ID Title

HPSBUX0202-184 Sec. Vulnerability in SNMP (rev. 1)

The documents are listed below.

Document ID: HPSBUX0202-184

Date Loaded: 20020214

Title: Sec. Vulnerability in SNMP (rev. 1)

TEXT

REVISED 01 HEWLETT-PACKARD COMPANY SECURITY BULLETIN: #0184,

Originally issued: 12 Feb. 2002

Last revised: 13 Feb. 2002

The information in the following Security Bulletin should be acted upon as soon as possible. Hewlett-Packard Company will not be liable for any consequences to any customer resulting from customer's

failure to fully implement instructions in this Security Bulletin as soon as possible.

PROBLEM: Vulnerabilities in SNMP request and trap handling.

PLATFORM: HP 9000 Series 700 and Series 800 running HP-UX releases 10.X and 11.X

** Revised 01**

HP Procurve switches

JetDirect Firmware (older versions only)

DAMAGE: Possible denial-of-service, service interruptions, unauthorized access.

SOLUTION: Apply patches or implement workarounds.

For HP-UX releases:

PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent

PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent

PSOV_03087 Solaris 2.X EMANATE Release 14.2

MANUAL ACTIONS: Upgrade or workaround action per below.

AVAILABILITY: Patches for some affected systems are available now.

CHANGE SUMMARY: Rev.01 affected HP Procurve scope expanded, plus Procurve patch availability added. NNM ovtrapd patch availability added.

A. Background

CERT has issued an advisory:

CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMPv1) containing information about the vulnerabilities.

Hewlett-Packard Company will revise this bulletin as new information becomes available.

hp Procurve switches

REVISED 01

We are still in the process of determining which other HP Procurve products are subject to these vulnerabilities.

We have created fixes for products below which will resolve these issues. See Section C below.

Customers can download these patches in the form of software upgrades at:

<http://www.hp.com/rnd/software/switches.htm>

Product Fix revision number

HP Procurve Switch 2524 (J4813A) F.04.08 or greater
HP Procurve Switch 2512 (J4812A) F.04.08 or greater
HP Procurve Switch 4108GL (J4865A) G.04.05 or greater
HP Procurve Switch 4108GL–bundle (J4861A) G.04.05 or greater

Not all HP Procurve products have completed testing, nor are they listed here, and may or may not have these vulnerabilities. This bulletin will again be updated as new information becomes available.

NNM (Network Node Manager)

****REVISED 01****

Some problems found in NNM product were related to trap handling. Patches are available. See Section C below.

JetDirect Firmware (older versions only)

ONLY some older versions of JetDirect Firmware are vulnerable to some of the issues. The older firmware can be upgraded in most cases, see list below.

JetDirect Firmware Version State

=====

X.08.32 and higher NOT Vulnerable
X.21.00 and higher NOT Vulnerable
where X represents an alpha character for your device.

JetDirect Product Numbers that can be freely upgraded to X.08.32 or X.21.00 or higher firmware.

EIO (Peripherals Laserjet 4000, 5000, 8000, etc...)

J3110A 10T
J3111A 10T/10B2/LocalTalk
J3112A Token Ring (discontinued)
J3113A 10/100 (discontinued)
J4169A 10/100
J4167A Token Ring

MIO (Peripherals LaserJet 4, 4si, 5si, etc...)

J2550A/B 10T (discontinued)
J2552A/B 10T/10Base2/LocalTalk (discontinued)
J2555A/B Token Ring (discontinued)
J4100A 10/100

J4105A Token Ring
J4106A 10T

External Print Servers
J2591A EX+ (discontinued)
J2593A EX+3 10T/10B2 (discontinued)
J2594A EX+3 Token Ring (discontinued)
J3263A 300X 10/100
J3264A 500X Token Ring
J3265A 500X 10/100

HP-UX Systems running snmpd or OPENVIEW

Any HP-UX 10.X or 11.X system running snmpd or snmpdm is vulnerable. To determine if your HP-UX system has snmpd or snmpdm installed:

```
swlist -l file | grep snmpd
```

B. Fixing the problem

Install the appropriate patch or firmware revision or work around problem as detailed below.

C. Recommended solution

hp Procurve switches

REVISED 01

Customers can download these patches in the form of firmware upgrades at:

<http://www.hp.com/rnd/software/switches.htm>

Product Fix revision number

HP Procurve Switch 2524 (J4813A) F.04.08 or greater
HP Procurve Switch 2512 (J4812A) F.04.08 or greater
HP Procurve Switch 4108GL (J4865A) G.04.05 or greater
HP Procurve Switch 4108GL-bundle (J4861A) G.04.05 or greater

NNM (Network Node Manager)

REVISED 01

Problems found in the NNM product (related only to trap handling) are addressed in patches available at:

http://support.openview.hp.com/cpe/patches/nnm/6.2/s700_800_11.X.jsp

PHSS_26286 s700_800 HP-UX 10.20 ovtrapd large trap fix
PHSS_26287 s700_800 HP-UX 11.X ovtrapd large trap fix

PSOV_03100 Solaris 2.X ovtrapd large trap fix
NNM_00857 NT 4.X/Windows 2000 ovtrapd large trap fix

MC/ServiceGuard

Concerning the impact of disabling the SNMP agent on nodes in MC/ServiceGuard or ServiceGuard OPS Edition clusters:

If SNMP is disabled on nodes running in MC/ServiceGuard or ServiceGuard OPS Edition clusters, it will no longer be possible for cluster monitoring applications that use the cluster SNMP MIB to obtain the correct status for the cluster.

Examples of such applications are ClusterView, ClusterView Plus or EMS High Availability Monitors, which all receive cluster-related SNMP information from the cluster nodes.

This means that these applications will no longer display the correct status for the cluster, including the cluster starting or halting, nodes leaving or joining the cluster, and application packages starting up or halting in the cluster.

NOTE: All supported versions of MC/ServiceGuard as well as ServiceGuard OPS Edition are affected by this issue.

The ServiceGuard Manager product does not use the cluster SNMP MIB, and therefore is NOT affected by the disabling of SNMP on cluster nodes.

Event Monitoring System (EMS)

It should also be noted that if an MC/ServiceGuard or ServiceGuard OPS Edition application package has package resources defined that use EMS High Availability Monitors, then those package resources will no longer contain the current status for the cluster. It may be necessary to remove the definition for these package resources in order to allow continued operation of the package after SNMP has been disabled.

JetDirect Firmware (older versions only)

Update firmware to X.08.32(or higher) or X.21.00(or higher) as applicable.

HP-UX Systems running snmpd or OPENVIEW

The following patches are available now:

PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent\$
PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent\$
PSOV_03087 Solaris 2.X EMANATE Release 14.2 \$

All three patches are available from:

<http://support.openview.hp.com/cpe/patches/>

Revised 01

-->> In addition PHSS_26137 and PHSS_26138 are now available from:

<http://itrc.hp.com>

=====
NOTE: The patches are labeled OV (Open View). However, the patches are also applicable to systems that are NOT running Open View.
=====

Workaround for HP-UX Systems:

If a patch is not available for your platform or you cannot install an available patch, snmpd and snmpdm can be disabled by removing their entries from /etc/services and removing the execute permissions from /usr/sbin/snmpd and /usr/sbin/snmpdm.

D. To subscribe to automatically receive future NEW HP Security Bulletins from the HP IT Resource Center via electronic mail, do the following:

Use your browser to get to the HP IT Resource Center page at:

<http://itrc.hp.com>

Use the 'Login' tab at the left side of the screen to login using your ID and password. Use your existing login or the "Register" button at the left to create a login, in order to gain access to many areas of the ITRC. Remember to save the User ID assigned to you, and your password.

In the left most frame select "Maintenance and Support".

Under the "Notifications" section (near the bottom of the page), select "Support Information Digests".

To ~~subscribe~~ to future HP Security Bulletins or other Technical Digests, click the check box (in the left column) for the appropriate digest and then click the "Update Subscriptions" button at the bottom of the page.

or

To –review– bulletins already released, select the link (in the middle column) "Search Technical Knowledge Database".

To –gain access– to the Security Patch Matrix, or the "The Security Bulletins Archive" select the link for "The Security Bulletins Archive" (near the bottom of the page). Once in the archive the third link is to the current Security Patch Matrix. Updated daily, this matrix categorizes security patches by platform/OS release, and by bulletin topic. Security Patch Check completely automates the process of reviewing the patch matrix for 11.XX systems.

For information on the Security Patch Check tool, see:
http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA"

The security patch matrix is also available via anonymous ftp:

ftp.itrc.hp.com:~ftp/export/patches/hp-ux_patch_matrix

On the "Support Information Digest Main" page:
click on the "HP Security Bulletin Archive".

E. To report new security vulnerabilities, send email to

security-alert@hp.com

Please encrypt any exploit information using the security-alert PGP key, available from your local key server, or by sending a message with a –subject– (not body) of 'get key' (no quotes) to security-alert@hp.com.

Permission is granted for copying and circulating this Bulletin to Hewlett-Packard (HP) customers (or the Internet community) for the purpose of alerting them to problems, if and only if, the Bulletin is not edited or changed in any way, is attributed to HP, and provided such reproduction and/or distribution is performed for non-commercial purposes.

Any other use of this information is prohibited. HP is not liable for any misuse of this information by any third party.

-----End of Document ID: HPSBUX0202-184-----

-----BEGIN PGP SIGNATURE-----

Version: PGP for Business Security 5.5

iQA/AwUBPG3obuAfOvwtKn1ZEqJ/rQCdFex4PXoP2bljyoJb8NSJO63ib78AoJ2y
2PrfoqoHqOLt53wZH5bYiV7g
=idJE

-----END PGP SIGNATURE-----

Yours truly,
HP S/W Security Team
WTEC Cupertino, California

Reply-to: security-alert@hp.com

--

- *Next message:* [Gavin Kerr: "Re: Microsoft finally acknowledges the security drumbeats"](#)
- *Previous message:* [Marty Fouts: "Re: Microsoft finally acknowledges the security drumbeats"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)