

Security Vulnerability SNMP (rev. 12)

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-10/1116.html>

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

Date: 07/10/02

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

Date: 10 Jul 2002 13:41:03 GMT

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

Hash: SHA1

****REVISED 12** HEWLETT-PACKARD COMPANY SECURITY BULLETIN: #0184,**
Originally issued: 12 Feb. 2002
Last revision: 10 July 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
HP Procurve switches
HP TopTools Remote Control Card
JetDirect Firmware
MC/ServiceGuard, EMS HA Monitors
Solaris running OpenView or NNM
Windows/NT running OpenView or NNM

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

SOLUTION: Apply patches or implement workarounds. See below.
For HP-UX releases:

PHSS_26510 s700_800 HP-UX 10.10, 10.01 Emanate 14.0
PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent
PHSS_27181 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent

comp.security.misc: Security Vulnerability SNMP (rev. 12)

PHSS_26367 s700_800 HP-UX 10.24 VirtualVault (VVOS)
PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent
PHSS_27182 s700_800 HP-UX 11.X OV EMANATE14.2 Agent
PHSS_26368 s700_800 HP-UX 11.04 VirtualVault (VVOS)

PSOV_03087 Solaris 2.5.1, Solaris 2.6, Solaris 2.7
Solaris 2.8 EMANATE Release 14.2

PSOV_03162 Solaris 2.5.1, Solaris 2.6, Solaris 2.7
Solaris 2.8 EMANATE Release 14.2

PSOV_03113 Solaris 2.3, Solaris 2.4 Emanate Release 14.0

For systems running OV NNM install above SNMP
patches for HP-UX and Solaris in addition to the NNM
patches listed below.

For Windows/NT install:

NNM_00846 Windows NT4.0/4.01 Windows 2000

NNM_00909 Windows NT4.0/4.01 Windows 2000

NNM6.2

PHSS_26932 NNM 6.2 HP-UX 10.20

PHSS_26933 NNM 6.2 HP-UX 11.X

NNM_00890 NNM 6.2 Win NT/2k

PSOV_03144 NNM 6.2 Solaris 2.X

NNM6.1 Note: both patches are required.

PHSS_26918, PHSS_26908 NNM 6.1 HP-UX 10.20

PHSS_26919, PHSS_26909 NNM 6.1 HP-UX 11.X

NNM_00889, ECS_00011 NNM 6.1 Win NT/2k

PSOV_03143, PSOV_03142 NNM 6.1 Solaris 2.5,
2.6, 2.7, 2.8

NNM5.01

PHSS_26806 NNM 5.01 HP-UX 10.20

PSOV_03136 NNM 5.01 Solaris 2.X

NNM4.11

PHSS_26777 NNM 4.11 HP-UX 10.20

PSOV_03132 NNM 4.11 Solaris 2.X

****REVISED 12****

--->> OpenView Distributed Management 5.03

--->> PHSS_27273 - HP-UX 10.X

--->> PHSS_27274 - HP-UX 11.X

--->> PSOV_03173 - Solaris 2.X

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.
Rev.02 SG and EMS found not vulnerable.
Rev.03 JetDirect vulnerability updated
Rev.04 NNM 5.X and VVOS patches, vulnerability note
for Solaris, and Windows NT.
Rev.05 VVOS patch ID typo.
Rev.06 Updating NNM 5.X section, HP OC SS7 added
Rev.07 Added OpenView product status list
Rev.08 Added NNM 5.01 and 4.11 patches for HP-UX
and Solaris
Rev.09 New NNM 6.1 and NNM 6.2 patches, additional
Emanate patches, and TopTools Remote
Control Card information
Rev.10 Additional Emanate and NNM patches.
Rev.11 PHSS_27181,PHSS_27182, are only found on:
<http://support.openview.hp.com/cpe/patches/>
-->>Rev.12 OpenView Distributed Management 5.03
patches added. Added pointer to HP Compaq
security advisory.

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

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.

HP TopTools Remote Control Card

TopTools Remote Control (TTRC) card, rev. 2.0. (product P1218A) has an SNMP MIB defect.

NNM (Network Node Manager)

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

JetDirect Firmware

JetDirect Firmware Version State

=====

- X.08.32 and lower VULNERABLE
(where X = A through K)
- X.21.00 and higher NOT vulnerable
(where X = L through P)

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
```

Other systems running OpenView or NNM

Solaris and Windows/NT systems running OpenView or NNM are vulnerable.

OpenView Product Status

NNM Vulnerable

Patches in process

Note:

Patches for NNM 6.2, NNM 6.1, NNM 5.01, NNM 4.11, and Emanate are complete.
Patches for NNM 5.02 and NNM 6.01 are in process.
NNM also ships Emanate SNMP Agents so patches for Emanate SNMP Agents should also be applied (See section "C. Recommended solution" below).

ITO/VPO/OVO on Vulnerable

Unix Patches in process

Note:

This product bundles the NNM and Emanate Agents with it. Appropriate NNM and Emanate Agent patches should also be applied. (See section "C. Recommended solution" below).

OVO Windows Under Investigation

VPW/OVO Windows Note:

OVO bundles the NNM and Emanate Agents with it. Appropriate NNM and Emanate agent patches should also be applied. (See section "C. Recommended solution" below).

Extensible Agent Vulnerable

(EA) Patches released

HP-UX 10.01, 10.10
– PHSS_26510
HP-UX 10.20 – PHSS_26137
HP-UX 11.0 – PHSS_26138
Solaris 2.5.1, 2.6, 2.7, 2.8
– PSOV_03087
Solaris 2.3, 2.4
– PSOV_03113

Emanate SNMP Agents Vulnerable

Patches released:

HP-UX 10.01, 10.10 – PHSS_26510
HP-UX 10.20 – PHSS_26137, PHSS_27181
HP-UX 11.X – PHSS_26138, PHSS_27182
Solaris 2.5.1, 2.6, 2.7, 2.8
– PSOV_03087, PSOV_03162
Solaris 2.3, 2.4

– PSOV_03113
NT – NNM_00846, NNM_00909

SAM builder Under Investigation

SAM allocator Under Investigation

SAM accountant Under Investigation

SAM optimizer Under Investigation

SAM SNM Under Investigation

SA (Service Assurance) Under Investigation

OEMF Under Investigation

****REVISED 12****

- -->> DM DM Release 5.03 Vulnerable.
 - -->> Patches released:
 - -->> PHSS_27273 – HP-UX 10.X
 - -->> PHSS_27274 – HP-UX 11.X
 - -->> PSOV_03173 – Solaris 2.X
 - -->> Other DM versions under
 - -->> investigation.
-

****REVISED 12****

- -->> Note: An HP Compaq security advisory (SSRT0799) is available
- -->> at <http://ftp.support.compaq.com/patches/.new/security.shtml>

B. Fixing the problem

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

C. Recommended solution

hp Procurve switches

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

NNM (Network Node Manager)

Problems found in the NNM 6.1 and NNM 6.2 products are addressed in patches available at:

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

Note: The NNM 6.2 patches listed in previous revisions of this bulletin only addressed trap handling. The following patches address all NNM 6.2 vulnerabilities.

PHSS_26932 s700_800 HP-UX 10.20 all fixes
PHSS_26933 s700_800 HP-UX 11.X all fixes
PSOV_03144 Solaris 2.X all fixes
NNM_00890 NT 4.X/Windows 2000 all fixes

PHSS_26918, PHSS_26908 NNM 6.1 HP-UX 10.20
PHSS_26919, PHSS_26909 NNM 6.1 HP-UX 11.X
NNM_00889, ECS_00011 NNM 6.1 Win NT/2k
PSOV_03143, PSOV_03142 NNM 6.1 Solaris 2.5,
2.6, 2.7, 2.8

Note: For NNM 6.1 both patches are required.

For NNM 5.01, and 4.11 (HP-UX and Solaris versions only) see the list below, and obtain the patches from:

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

NNM 5.01

HP-UX 10.20 PHSS_26806
Solaris 2.X PSOV_03136

NNM 4.11

HP-UX 10.20 PHSS_26777
Solaris 2.X PSOV_03132

Patches for NNM 5.02 and NNM 6.01 are in process.
This bulletin will be updated when new patches are available.

****REVISED 12****

-->> DM (OpenView Distributed Management)

-->> Problems found in the OpenView Distributed Management 5.03
-->> are addressed in patches available at:

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

- >> PHSS_27273 – HP-UX 10.X
- >> PHSS_27274 – HP_UX 11.X
- >> PSOV_03173 – Solaris 2.X

MC/ServiceGuard

MC/ServiceGuard is not affected. Testing has been completed and neither MC/ServiceGuard nor ServiceGuard OPS Edition are negatively impacted.

The ServiceGuard Manager product does not use the cluster SNMP and remains unaffected.

Event Monitoring System (EMS)

Testing of the MC/ServiceGuard or ServiceGuard OPS Edition application with package resources defined using EMS High Availability Monitors has been completed and shows no vulnerability to this issue.

HP TopTools Remote Control Card

TopTools Remote Control (TTRC) card, rev. 2.0. (product P1218A) has an SNMP MIB defect. This is fixed in firmware version B.03.02 available at:

http://h20004.www2.hp.com/keeper_rnotes/bsdmatrix/matrix62319.html

JetDirect Firmware

JetDirect Firmware Version State

=====

X.08.32 and lower VULNERABLE
(where X = A through K)

X.21.00 and higher NOT vulnerable
(where X = L through P)

FIX STATUS: HP is working on a firmware fix.

WORKAROUND: Change the set-community-name and use the Access Control List as described in "HP JetDirect Print Servers – Making HP JetDirect Print Servers Secure on the Network":

http://www.hp.com/cposupport/networking/support_doc/bpj05999.html#P88_10129

LIMITING THE VULNERABILITY

SNMPv1 security relies on the set community name. It is important that a set-community-name be configured on the JetDirect device and that it be kept secret.

JetDirect Print Servers offer an Access Control List that can be used to specify which hosts can make SNMP configuration changes to JetDirect Print Servers.

The steps above can help prevent exploitation of the vulnerability. To eliminate the vulnerability before a fix is available SNMP can be disabled on the JetDirect device.

DISABLING SNMP ON A JETDIRECT PRINT SERVER

1. Update the firmware to the highest level as described in the JetDirect Upgrade Instructions document:

http://www.hp.com/cposupport/networking/support_doc/bpj06917.html

NOTE: Disabling SNMP may affect device discovery and port monitors that use SNMP to get status on the device. Use this feature with care.

2. Telnet to the JetDirect device (on the latest firmware) and type:

```
snmp-config: 0  
quit
```

This will completely disable SNMP on the JetDirect device.

HP always recommends upgrading JetDirect firmware for the latest bug fixes and security benefits. The upgrade firmware and download utility are available free of charge:

http://www.hp.com/cposupport/networking/support_doc/bpj06917.html

The following is a list of JetDirect Product Numbers that can be freely upgraded to X.08.32 or X.21.00 or higher firmware. The latest firmware revision available for download is given. For example, the latest firmware revision for the J3110A is G.08.32.

EIO (Peripherals LaserJet 4000, 5000, 8000, etc...)
J3110A 10T [G.08.32]
J3111A 10T/10B2/LocalTalk [G.08.32]

J3112A Token Ring (discontinued) [G.08.32]
J3113A 10/100 (discontinued) [G.08.32]
J4169A 10/100 [L.21.22]
J4167A Token Ring [L.21.25]
J6057A 10/100 [R.22.09]

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

J2550A/B 10T (discontinued) [A.08.32]
J2552A/B 10T/10Base2/LocalTalk (discontinued) [A.08.32]
J2555A/B Token Ring (discontinued) [A.08.32]
J4100A 10/100 [K.08.32]
J4105A Token Ring [K.08.32]
J4106A 10T [K.08.32]

LIO (Peripherals Color InkJet cp1160, cp1700)

J6042A 250m 10/100 [N.21.22]

External Print Servers

J2591A EX+ (discontinued) [E.08.32]
J2593A EX+3 10T/10B2 (discontinued) [D.08.32]
J2594A EX+3 Token Ring (discontinued) [D.08.32]
J3263A 300X 10/100 [H.08.32]
J3264A 500X Token Ring [J.08.32]
J3265A 500X 10/100 [J.08.32]
J6038A 310x USB 10/100 [Q.22.04]

HP-UX Systems running snmpd or OpenView

The following patches are available now:

PHSS_26510 s700_800 HP-UX 10.10, 10.01 Emanate 14.0
PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent
PHSS_27181 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent
PHSS_26367 s700_800 HP-UX 10.24 VirtualVault (VVOS)
PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent
PHSS_27182 s700_800 HP-UX 11.X OV EMANATE14.2 Agent
PHSS_26368 s700_800 HP-UX 11.04 VirtualVault (VVOS)

PSOV_03087 Solaris 2.5.1, Solaris 2.6, Solaris 2.7
Solaris 2.8 EMANATE Release 14.2
PSOV_03162 Solaris 2.5.1, Solaris 2.6, Solaris 2.7
Solaris 2.8 EMANATE Release 14.2
PSOV_03113 Solaris 2.3, Solaris 2.4 Emanate Release 14.0

For systems running OV NNM install above SNMP
patches for HP-UX and Solaris.

For Windows/NT install:

NNM_00846 Windows NT4.0/4.01 Windows 2000

NNM_00909 Windows NT4.0/4.01 Windows 2000

PSOV_03087, PSOV_0162, NNM_00846, NNM_00909, PSOV_03113,
PHSS_27181, PHSS_27182 are available from:

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

PHSS_26367 and PHSS_26368 available from:

<http://itrc.hp.com>

PHSS_26510, PHSS_26137, and PHSS_26138 are available
from both sites.

The HP OC SS7 (OpenCall) products J3362A and J5938A running
on HP-UX releases 10.20 and 11.X are not vulnerable if the
applicable HP-UX patch listed above is installed.

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

Workaround for HP-UX Systems:

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

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) for the appropriate digest.

To –gain access– to the Security Patch Matrix, 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.

-----BEGIN PGP SIGNATURE-----
Version: PGP Personal Security 7.0.3

comp.security.misc: Security Vulnerability SNMP (rev. 12)

iQA/AwUBPSw3auAfOvwtKn1ZEqJr2gCfTO9I7dLptz7Xz6u0rG0PhPKNnXwAoLUF
+VcblnL0hKAIKII6/7fftyF3
=McXa
-----END PGP SIGNATURE-----

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

Return-Path: secure@cup.hp.com Reply-to: security-alert@hp.com

- **Next message:** [Security Alert: "Security Vulnerability ASUnetbios"](#)
- **Previous message:** [john.veldhuis@universal.nl: "Re: Confirmed Cases Of Trapdoors By Overseas Programmers ?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)