

[security bulletin] HPSBMA02242 SSRT061260 rev.3 – HP OpenView Network Node Manager (OV NNM) Running Shared Trace Service, Remote Arbitrary Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-04/msg00085.html>

- *From:* security-alert@xxxxxx
 - *Date:* Tue, 08 Apr 2008 11:04:14 -0700
-

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

Hash: SHA1

SUPPORT COMMUNICATION – SECURITY BULLETIN

Document ID: c01112038

Version: 3

HPSBMA02242 SSRT061260 rev.3 – HP OpenView Network Node Manager (OV NNM) Running Shared Trace Service, Remote Arbitrary Code Execution

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

Release Date: 2007-08-07

Last Updated: 2008-04-08

Potential Security Impact: Remote arbitrary code execution

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

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM) running Shared Trace Service. The vulnerability could be remotely exploited to execute arbitrary code.

References: CVE-2007-3872

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP OpenView Network Node Manager (OV NNM) v6.41, v7.01, v7.50, v7.51 running XPL earlier than 03.10.040 on HP-UX, Solaris, Windows NT, Windows 2000, Windows XP, and Linux

BACKGROUND

CVSS 2.0 Base Metrics

=====

Reference Base Vector Base Score

CVE-2007-3872 (AV:N/AC:M/Au:N/C:P/I:P/A:P) 6.8

=====

Information on CVSS is documented in HP Customer Notice: HPSN-2008-002.

The Hewlett-Packard Company thanks Cody Pierce of TippingPoint DV Labs (dvlabs.tippingpoint.com) for reporting this vulnerability to security-alert@xxxxxxx

The Hewlett-Packard Company thanks an anonymous researcher working with the iDefense VCP for reporting this vulnerability to security-alert@xxxxxxx

RESOLUTION

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

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

Note: The software patches listed below require CME Component Bundles. The required CME Component Bundle is specified in the patch documentation for each patch. The specified CME Component Bundle is necessary to resolve the vulnerability.

OV NNM v7.51

HP-UX (PA)

PHSS_36901 or subsequent

HP-UX (IA)

PHSS_36902 or subsequent

Solaris

PSOV_03482 or subsequent

Windows 2000, Windows XP

NNM_01161 or subsequent

Linux RedHatAS2.1

LXOV_00054 or subsequent

OV NNM v7.50

HP-UX (PA)

Upgrade to NNM v7.51 and install PHSS_36901 or subsequent

HP-UX (IA)

Upgrade to NNM v7.51 and install PHSS_36902 or subsequent

Solaris

Upgrade to NNM v7.51 and install PSOV_03482 or subsequent

Windows 2000, Windows XP

Upgrade to NNM v7.51 and install NNM_01161 or subsequent

Linux RedHatAS2.1

Upgrade to NNM v7.51 and install LXOV_00054 or subsequent

OV NNM v7.01

HP-UX (PA)

PHSS_36773 or subsequent

Solaris

PSOV_03480 or subsequent

Windows 2000, Windows XP

NNM_01159 or subsequent

OV NNM v6.41

HP-UX (PA)

PHSS_37141 or subsequent

Solaris

PSOV_03489 or subsequent

Windows 2000, Windows XP

NNM_01167 or subsequent

MANUAL ACTIONS: Yes – NonUpdate

For HP-UX OV NNM 7.50 – Upgrade to NNM 7.51 and install the appropriate patch

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 Security Bulletins issued by HP 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>

The following text is for use by the HP-UX Software Assistant.

AFFECTED VERSIONS (for HP-UX)

For HP-UX OV NNM 7.51

HP-UX B.11.31

HP-UX B.11.23 (IA)

=====

OVNNMgr.OVNNM-RUN

action: install PHSS_36902 or subsequent

URL: <http://itrc.hp.com>

HP–UX B.11.23 (PA)

HP–UX B.11.11

HP–UX B.11.00

=====

OVNNMgr.OVNNM–RUN

action: install PHSS_36901 or subsequent

URL: <http://itrc.hp.com>

For HP–UX OV NNM 7.50

HP–UX B.11.23

=====

OVNNMgr.OVNNM–RUN action:

action: install revision 7.51 or subsequent

For HP–UX OV NNM 7.01

HP–UX B.11.00

HP–UX B.11.11

=====

OVNNMgr.OVNNM–RUN

action: install PHSS_36773 or subsequent

URL: <http://itrc.hp.com>

For HP–UX OV NNM 6.41

HP–UX B.11.00

HP–UX B.11.11

=====

OVNNMgr.OVNNM–RUN

action: install PHSS_37141 or subsequent

URL: <http://itrc.hp.com>

END AFFECTED VERSIONS (for HP–UX)

HISTORY

Version: 1 (rev.1) – 7 August 2007 Initial release

Version: 2 (rev.2) – 16 August 2007 Added NNM v7.51

Version: 3 (rev.3) – 8 April 2008 Patches available

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

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

Report: To report a potential security vulnerability with any HP supported product, send Email to: security–alert@xxxxxx

It is strongly recommended that security related information being communicated to HP be encrypted using PGP, especially exploit information.

To get the security–alert PGP key, please send an e–mail message as follows:

To: security–alert@xxxxxx

Subject: get key

Subscribe: To initiate a subscription to receive future HP Security Bulletins via Email:

http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in_SC-GEN_driv

On the web page: ITRC security bulletins and patch sign-up

Under Step1: your ITRC security bulletins and patches

– check ALL categories for which alerts are required and continue.

Under Step2: your ITRC operating systems

– verify your operating system selections are checked and save.

To update an existing subscription: <http://h30046.www3.hp.com/subSignIn.php>

Log in on the web page: Subscriber's choice for Business: sign-in.

On the web page: Subscriber's Choice: your profile summary – use Edit Profile to update appropriate sections.

To review previously published Security Bulletins visit:

<http://www.itrc.hp.com/service/cki/secBullArchive.do>

* The Software Product Category that this Security Bulletin relates to is represented by the 5th and 6th characters of the Bulletin number in the title:

GN = HP General SW

MA = HP Management Agents

MI = Misc. 3rd Party SW

MP = HP MPE/iX

NS = HP NonStop Servers

OV = HP OpenVMS

PI = HP Printing & Imaging

ST = HP Storage SW

TL = HP Trusted Linux

TU = HP Tru64 UNIX

UX = HP-UX

VV = HP VirtualVault

System management and security procedures must be reviewed frequently to maintain system integrity. HP is continually reviewing and enhancing the security features of software products to provide customers with current secure solutions.

"HP is broadly distributing this Security Bulletin in order to bring to the attention of users of the affected HP products the important security information contained in this Bulletin. HP recommends that all users determine the applicability of this information to their individual situations and take appropriate action. HP does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, HP will not be responsible for any damages resulting from user's use or disregard of the information provided in this Bulletin. To the extent permitted by law, HP disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non-infringement."

©Copyright 2008 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HP or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein are trademarks of Hewlett-Packard Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.

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

Version: PGP 8.1

iQA/AwUBR/uN+eAfOvwtKn1ZEQIpHACcDbLTAo/ahxr9y8UGxfug5gtn3EIAoPBd
bTyxCxt6YgrBhXqgSzKgUxK1
=0Sy1

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