

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [bugtraq](#)
Subject: [security bulletin] HPSBMU02797 SSRT100867 rev.1 - HP Network Node Manager i (NNMi) v9.1x I
From: [security-alert\(.\)hp ! com](#)
Date: [2012-07-17 13:06:52](#)
Message-ID: [20120717130652.AC15120925\(.\)_security ! hp ! com](#)
[Download RAW [message](#) or [body](#)]

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

Hash: SHA1

Note: the current version of the following document is available here:

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c03358587

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c03358587
Version: 1

HPSBMU02797 SSRT100867 rev.1 - HP Network Node Manager i (NNMi) v9.1x Running
JDK for HP-UX, Linux, Solaris, and Windows, Remote Unauthorized Information
Disclosure, Modification, Denial of Service (DoS)

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

Release Date: 2012-07-16
Last Updated: 2012-07-16

Potential Security Impact: Remote unauthorized information disclosure, modification, Denial of Service (DoS)

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

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified with HP Network Node Manager I (NNMi) running JDK for HP-UX, Linux, Solaris, and Windows. The vulnerabilities could be remotely exploited resulting in unauthorized information disclosure, modification, Denial of Service (DoS).

References: CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4450, CVE-2010-4451, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4469, CVE-2010-4470, CVE-2010-4471, CVE-2010-4472, CVE-2010-4473, CVE-2010-4474, CVE-2010-4475, CVE-2010-4476, CVE-2011-0786, CVE-2011-0788, CVE-2011-0802, CVE-2011-0814, CVE-2011-0815, CVE-2011-0817, CVE-2011-0862, CVE-2011-0863, CVE-2011-0864, CVE-2011-0865, CVE-2011-0866, CVE-2011-0867, CVE-2011-0868, CVE-2011-0869, CVE-2011-0871, CVE-2011-0872, CVE-2011-0873, CVE-2011-3389, CVE-2011-3516, CVE-2011-3521, CVE-2011-3544, CVE-2011-3545, CVE-2011-3546, CVE-2011-3547, CVE-2011-3548, CVE-2011-3549, CVE-2011-3550, CVE-2011-3551, CVE-2011-3552, CVE-2011-3553, CVE-2011-3554, CVE-2011-3555, CVE-2011-3556, CVE-2011-3557, CVE-2011-3558, CVE-2011-3560, CVE-2011-3561, CVE-2011-3563, CVE-2011-5035, CVE-2012-0497, CVE-2012-0498, CVE-2012-0499, CVE-2012-0500, CVE-2012-0501, CVE-2012-0502, CVE-2012-0503, CVE-2012-0504, CVE-2012-0505, CVE-2012-0506, CVE-2012-0507, CVE-2012-0508

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Network Node Manager I (NNMi) v9.1x for HP-UX, Linux, Solaris, and Windows

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2010-4422	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2010-4447	(AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3
CVE-2010-4448	(AV:N/AC:H/Au:N/C:N/I:P/A:N)	2.6
CVE-2010-4450	(AV:L/AC:H/Au:N/C:P/I:P/A:P)	3.7
CVE-2010-4451	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2010-4452	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4454	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4462	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4463	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4465	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4466	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2010-4467	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4468	(AV:N/AC:H/Au:N/C:P/I:P/A:N)	4.0
CVE-2010-4469	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0

CVE-2010-4470	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2010-4471	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2010-4472	(AV:N/AC:H/Au:N/C:N/I:N/A:P)	2.6
CVE-2010-4473	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2010-4474	(AV:L/AC:L/Au:N/C:P/I:N/A:N)	2.1
CVE-2010-4475	(AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3
CVE-2010-4476	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2011-0786	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2011-0788	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2011-0802	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0814	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0815	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0817	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0862	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0863	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0864	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0865	(AV:N/AC:H/Au:N/C:N/I:P/A:N)	2.6
CVE-2011-0866	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2011-0867	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2011-0868	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2011-0869	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2011-0871	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-0872	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2011-0873	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3389	(AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3
CVE-2011-3516	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2011-3521	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3544	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3545	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3546	(AV:N/AC:M/Au:N/C:P/I:P/A:N)	5.8
CVE-2011-3547	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2011-3548	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3549	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3550	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2011-3551	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	9.3
CVE-2011-3552	(AV:N/AC:H/Au:N/C:N/I:P/A:N)	2.6
CVE-2011-3553	(AV:N/AC:M/Au:S/C:P/I:N/A:N)	3.5
CVE-2011-3554	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2011-3555	(AV:N/AC:H/Au:N/C:N/I:P/A:C)	6.1
CVE-2011-3556	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5
CVE-2011-3557	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	6.8
CVE-2011-3558	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2011-3560	(AV:N/AC:L/Au:N/C:P/I:P/A:N)	6.4
CVE-2011-3561	(AV:A/AC:H/Au:N/C:P/I:N/A:N)	1.8
CVE-2011-3563	(AV:N/AC:L/Au:N/C:P/I:N/A:P)	6.4
CVE-2011-5035	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2012-0497	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-0498	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-0499	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-0500	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-0501	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2012-0502	(AV:N/AC:L/Au:N/C:P/I:N/A:P)	6.4
CVE-2012-0503	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5
CVE-2012-0504	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	9.3
CVE-2012-0505	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5
CVE-2012-0506	(AV:N/AC:M/Au:N/C:N/I:P/A:N)	4.3
CVE-2012-0507	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-0508	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0

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

RESOLUTION

HP has made hotfixes available to resolve these vulnerabilities for NNMi v9.1x. The hotfixes can be obtained by contacting the normal HP Services support channel. Customers should open a support case to request the following hotfixes.

NNMi Version / Operating System

Required Patch
Hotfix

9.1x HP-UX

Patch 4
Hotfix-NNMi-9.1xP4-HP-UX-JDK-20120710.zip

9.1x Linux

Patch 4
Hotfix-NNMi-9.1xP4-Linux-JDK-20120523.zip

9.1x Solaris**Patch 4****Hotfix-NNMi-9.1xP4-Solaris-JDK-20120523.zip****9.1x Windows****Patch 4****Hotfix-NNMi-9.1xP4-Windows-JDK-20120523.zip**

Note: The hotfix must be installed after the required patch. The hotfix must be reinstalled if the required patch is reinstalled.

MANUAL ACTIONS: Yes - Update

Install the applicable patch and hotfix.

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 NNMi v9.1x

HP-UX B.11.31

HP-UX B.11.23 (IA)

=====

HPOVNNM.HPOVNNMUI

action: install Hotfix-NNMi-9.1xP4-HP-UX-JDK-20120710.zip

END AFFECTED VERSIONS**HISTORY**

Version:1 (rev.1) - 16 July 2012 Initial release

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

Support: For issues about implementing the recommendations of this Security Bulletin, contact normal HP Services support channel. For other issues about the content of this Security Bulletin, send e-mail to security-alert@hp.com.

Report: To report a potential security vulnerability with any HP supported product, send Email to: security-alert@hp.com

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

http://h41183.www4.hp.com/signup_alerts.php?jumpid=hpsec_bulletins

Security Bulletin List: A list of HP Security Bulletins, updated periodically, is contained in HP Security Notice HPSN-2011-001:

https://h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c02964430

Security Bulletin Archive: A list of recently released Security Bulletins is available here:

<http://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive/>

Software Product Category: The Software Product Category is represented in the title by the two characters following HPSB.

3C = 3COM

3P = 3rd Party Software

GN = HP General Software

HF = HP Hardware and Firmware

MP = MPE/iX

MU = Multi-Platform Software

NS = NonStop Servers

OV = OpenVMS

PI = Printing and Imaging

PV = ProCurve

ST = Storage Software

TU = Tru64 UNIX

UX = HP-UX

Copyright 2012 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: GnuPG v1.4.10 (GNU/Linux)

iEYEARECAAYFA1AELpsACgkQ4B86/C0qfV1GNQCfVzWjPNz+NmZLGDFK6Qdyaovs
7f8An2XqqESp6ptuRfb33heTfEsZ2h7I
=4j6W

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

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)