

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

List: [bugtraq](#)
Subject: [security bulletin] HPSBUX02784 SSRT100871 rev.1 - HP-UX Running Java, Remote Unauthorized
From: [security-alert\(.\)hp!com](#)
Date: [2012-05-31 2:02:42](#)
Message-ID: [20120531020242.B635120804\(.\)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-c03350339

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c03350339
Version: 1

HPSBUX02784 SSRT100871 rev.1 - HP-UX Running Java, Remote Unauthorized
Access, Disclosure of Information, and Other Vulnerabilities

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

Release Date: 2012-05-30
Last Updated: 2012-05-29

Potential Security Impact: Remote unauthorized access, disclosure of
information, and other vulnerabilities

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

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified in Java Runtime
Environment (JRE) and Java Developer Kit (JDK) running on HP-UX. These
vulnerabilities could allow remote unauthorized access, disclosure of
information, and other vulnerabilities.

References: 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

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.23, B.11.31 running HP JDK and JRE 7.0.0

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
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

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

RESOLUTION

HP has provided the following Java version upgrade to resolve these
vulnerabilities.
The upgrade is available from the following location

<http://www.hp.com/go/java>

HP-UX B.11.23, B.11.31

JDK and JRE v7.0.01 or subsequent

MANUAL ACTIONS: Yes - Update

For Java v7.0.0, update to Java v7.0.01 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 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

HP-UX B.11.23

HP-UX B.11.31

=====

Jdk70.JDK70-COM

Jdk70.JDK70-DEMO

Jdk70.JDK70-IPF32

Jdk70.JDK70-IPF64

Jre70.JRE70-COM

Jre70.JRE70-IPF32

Jre70.JRE70-IPF32-HS

Jre70.JRE70-IPF64

Jre70.JRE70-IPF64-HS

action: install revision 1.7.0.01 or subsequent

END AFFECTED VERSIONS

HISTORY

Version:1 (rev.1) 30 May 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=hpsecbulletins

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

[docDisplay?docId=emr_na-c02964430](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)

iEYEARECAAYFAk/Gu24ACgkQ4B86/C0qfVng9ACg6wMvjSRvXh5zW4MfqUMeui5e
F9sAn04CEax2mTk8EraASTn8mFKee0lo
=tRJJu

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

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

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