[prev in list] [next in list] [prev in thread] [next in thread]

List: bugtraq
Subject: [security bulletin] HPSBUX02857 SSRT101103 rev.1 - HP-UX Running Java, Remote Unauthorized
From: security-alert () hp ! com
Date: 2013-03-26 18:30:52
Message-ID: 20130326183052.DC5BA201B2 () 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-c03714148

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c03714148
Version: 1

HPSBUX02857 SSRT101103 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: 2013-03-25
Last Updated: 2013-03-22

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 exploits.

References: CVE-2012-1541, CVE-2012-3213, CVE-2012-3342, CVE-2013-0169,
CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424,
CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0429,
CVE-2013-0431, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435,
CVE-2013-0437, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442,
CVE-2013-0443, CVE-2013-0444, CVE-2013-0445, CVE-2013-0446, CVE-2013-0449,
CVE-2013-0450, CVE-2013-0809, CVE-2013-1473, CVE-2013-1475, CVE-2013-1476,
CVE-2013-1478, CVE-2013-1480, CVE-2013-1484, CVE-2013-1485, CVE-2013-1486,
CVE-2013-1487, CVE-2013-1489, CVE-2013-1493

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.23, and B.11.31 running HP JDK and JRE v7.0.04 and earlier

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2012-1541	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-3213	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2012-3342	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2013-0169	(AV:N/AC:H/Au:N/C:P/I:N/A:N)	2.6
CVE-2013-0351	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5
CVE-2013-0409	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2013-0419	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2013-0423	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2013-0424	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2013-0425	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2013-0426	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2013-0427	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2013-0428	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2013-0429	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6
CVE-2013-0431	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2013-0432	(AV:N/AC:L/Au:N/C:P/I:P/A:N)	6.4
CVE-2013-0433	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2013-0434	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2013-0435	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	5.0
CVE-2013-0437	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10.0
CVE-2013-0438	(AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3

```
CVE-2013-0440    (AV:N/AC:L/Au:N/C:N/I:N/A:P)        5.0
CVE-2013-0441    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0442    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0443    (AV:N/AC:H/Au:N/C:P/I:P/A:N)        4.0
CVE-2013-0444    (AV:N/AC:H/Au:N/C:C/I:C/A:C)        7.6
CVE-2013-0445    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0446    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0449    (AV:N/AC:L/Au:N/C:P/I:N/A:N)        5.0
CVE-2013-0450    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0809    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1473    (AV:N/AC:L/Au:N/C:N/I:P/A:N)        5.0
CVE-2013-1475    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1476    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1478    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1480    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1484    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1485    (AV:N/AC:L/Au:N/C:N/I:P/A:N)        5.0
CVE-2013-1486    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1487    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1489    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1493    (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/java

HP-UX B.11.23, B.11.31
 JDK and JRE v7.0.05 or subsequent

MANUAL ACTIONS: Yes - Update
For Java v7.0 update to Java v7.0.05 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 1.7.0.04.00 or subsequent

END AFFECTED VERSIONS

HISTORY
Version:1 (rev.1) - 25 March 2013 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=hpsc_secbulletins

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

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.13 (GNU/Linux)

iEYEARECAAYFAlFQwqcACgkQ4B86/C0qfVkdswCg5QlaRop7wSZnjOkQltgbef0J
UbIAn2QdxK84jBaE8XmcZEPI/9mVdiBd
=L4Fp
-----END PGP SIGNATURE-----

[prev in list] [next in list] [prev in thread] [next in thread]

Configure | About | News | Add a list | Sponsored by KoreLogic