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

List: bugtraq
Subject: [security bulletin] HPSBMU02874 SSRT101184 rev.1 - HP Service Manager, Java Runtime Enviro
From: security-alert () hp ! com
Date: 2013-04-29 16:23:40
Message-ID: 20130429162340.B19AE20401 () 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-c03748879

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c03748879
Version: 1

HPSBMU02874 SSRT101184 rev.1 - HP Service Manager, Java Runtime Environment
(JRE) Security Update

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

Release Date: 2013-04-29
Last Updated: 2013-04-29

Potential Security Impact: Java Runtime Environment (JRE) security update

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

VULNERABILITY SUMMARY
Several potential security vulnerabilities have been identified with HP
Service Manager for Windows, Linux, HP-UX, Solaris and AIX. The Java Runtime
Environment (JRE) has been updated to correct these issues.

References: CVE-2013-1487, CVE-2013-1486,
CVE-2013-1484,CVE-2013-1485,CVE-2013-0169, CVE-2013-0437, CVE-2013-1478,
CVE-2013-0442, CVE-2013-0445, CVE-2013-1480, CVE-2013-0441, CVE-2013-1475,
CVE-2013-1476, CVE-2012-1541, CVE-2013-0446, CVE-2012-3342, CVE-2013-0450,
CVE-2013-1479, CVE-2013-0425, CVE-2013-0426, CVE-2013-0428, CVE-2012-3213,
CVE-2013-1481, CVE-2013-0436, CVE-2013-0439, CVE-2013-0447, CVE-2013-1472,
CVE-2012-4301, CVE-2013-1477, CVE-2013-1482, CVE-2013-1483, CVE-2013-1474,
CVE-2012-4305, CVE-2013-0444, CVE-2013-0429, CVE-2013-0419, CVE-2013-0423,
CVE-2012-1543, CVE-2013-0351, CVE-2013-0430, CVE-2013-0432, CVE-2013-0449,
CVE-2013-1473, CVE-2013-0435, CVE-2013-0434, CVE-2013-0409, CVE-2013-0431,
CVE-2013-0427, CVE-2013-0448, CVE-2013-0433, CVE-2013-0424, CVE-2013-0440,
CVE-2013-0438, CVE-2013-0443, CVE-2013-1489

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Service Manager for Windows, Linux, HP-UX, Solaris and AIX v 9.30, v9.31

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-2012-1543   (AV:N/AC:H/Au:N/C:C/I:C/A:C)   7.6
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-2012-4301   (AV:N/AC:L/Au:N/C:C/I:C/A:C)   10.0
CVE-2012-4305   (AV:N/AC:M/Au:N/C:C/I:C/A:C)   9.3
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-2013-0430   (AV:L/AC:M/Au:N/C:C/I:C/A:C)   6.9
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-2013-0436    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
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-2013-0439    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
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-2013-0447    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-0448    (AV:N/AC:L/Au:N/C:N/I:P/A:N)        5.0
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-2013-1472    (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-2013-1474    (AV:N/AC:M/Au:N/C:C/I:C/A:C)        9.3
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-2013-1477    (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-2013-1479    (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-2013-1481    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1482    (AV:N/AC:L/Au:N/C:C/I:C/A:C)       10.0
CVE-2013-1483    (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
==========================================================
             Information on CVSS is documented
            in HP Customer Notice: HPSN-2008-002

RESOLUTION

HP has provided an update for Service Manager that updates the JRE to the
latest version, thus eliminating known JRE7-related security vulnerabilities.
Download and install the updates from The HP Software Support Online (SSO).

SM 9.31P2 Server Windows Server 9.31.2004 p2
 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00423

HP Itanium Server 9.31.2004 p2
 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00420

Linux Server 9.31.2004 p2
 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00421

Solaris Server 9.31.2004 p2
 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00422

AIX Server 9.31.2004 p2
 http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00419

SM 9.31P2 Web Tier
Web Tier 9.31.2004 p2
http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00424

SM 9.31P2 Windows Client
Windows Client 9.31.2004 p2
http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00425

SM 9.31P2 Knowledge Management
SM 9.31P2 Knowledge Management
http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_HPSM_00426

HISTORY
Version:1 (rev.1) - 29 April 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)

iEYEARECAAYFAlF+g8UACgkQ4B86/C0qfVmutgCgmMLzjNXYunXplrMUfzTtKl7i
IOAAoK1RQj66CsQzz/QBmjwPLGfpTciZ
=rslo
-----END PGP SIGNATURE-----

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

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