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

List: bugtraq
Subject: [security bulletin] HPSBUX03188 SSRT101487 rev.1 - HP-UX running HP Secure Shell, Remote D
From: security-alert () hp ! com
Date: 2014-11-11 18:44:37
Message-ID: 20141111184437.355571FF1E () 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://h20564.www2.hp.com/portal/site/hpsc/public/kb/
docDisplay?docId=emr_na-c04499681

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04499681
Version: 1

HPSBUX03188 SSRT101487 rev.1 - HP-UX running HP Secure Shell, Remote Denial
of Service (DoS) and other Vulnerabilities

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

Release Date: 2014-11-07
Last Updated: 2014-11-07

Potential Security Impact: Remote Denial of Service (DoS) and other
vulnerabilities

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP-UX running HP
Secure Shell. These vulnerabilities could be exploited remotely to create a
Denial of Service (DoS) and other vulnerabilities.

References:

CVE-2013-4548 - remote Permissions, Privileges, and Access Control (CWE-264)

CVE-2014-1692 - remote Denial of Service (DoS), Buffer Errors (CWE-119)

CVE-2014-2532 - remote Permissions, Privileges, and Access Control (CWE-264)

CVE-2014-2653 - remote Input Validation (CWE-20)

SSRT101487

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11 running HP Secure Shell before version A.06.20.010

HP-UX B.11.23 running HP Secure Shell before version A.06.20.011

HP-UX B.11.31 running HP Secure Shell before version A.06.20.012

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2013-4548	(AV:N/AC:M/Au:S/C:P/I:P/A:P)	6.0
CVE-2014-1692	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5
CVE-2014-2532	(AV:N/AC:M/Au:N/C:P/I:P/A:N)	5.8
CVE-2014-2653	(AV:N/AC:M/Au:N/C:P/I:P/A:N)	5.8

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

RESOLUTION

HP has provided the following software updates to resolve this vulnerability.
The updates are available for download from:
http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=
T1471AA

OS Release

```
 HP Secure Shell Version
 Depot Name

HP-UX B.11.11 (11i v1)
 A.06.20.010 or subsequent
 HP_UX_11i_v1_T1471AA_A.06.20.010_HP-UX_B.11.11_32_64.depot

HP-UX B.11.23 (11i v2)
 A.06.20.011 or subsequent
 HP_UX_11i_v2_T1471AA_A.06.20.011_HP-UX_B.11.23_IA_PA.depot

HP-UX B.11.31 (11i v3)
 A.06.20.012 or subsequent
 HP_UX_11i_v3_SecureShell_A.06.20.012_HP-UX_B.11.31_IA_PA.depot

MANUAL ACTIONS: Yes - Update

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 HP-issued Security Bulletins 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

AFFECTED VERSIONS

HP-UX B.11.11
==============
Secure_Shell.SECURE_SHELL
action: install revision A.06.20.010 or subsequent

HP-UX B.11.23
==============
Secure_Shell.SECSH-CMN
Secure_Shell.SECURE_SHELL
action: install revision A.06.20.011 or subsequent

HP-UX B.11.31
==============
Secure_Shell.SECSH-CMN
Secure_Shell.SECURE_SHELL
action: install revision A.06.20.012 or subsequent

END AFFECTED VERSIONS

HISTORY: Version:1 (rev.1) - 7 November 2014 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 Archive: A list of recently released Security Bulletins is
available here:
https://h20564.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)

iEYEARECAAYFAlRdO/EACgkQ4B86/C0qfVnYkgCeLMLjqzE6VGLCkM3u78b26zM1
fb0AoP1SzrPW/A7s5xQwcYjlVEYxqxvL
=ZG0w
-----END PGP SIGNATURE-----

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

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