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

List: bugtraq
Subject: [security bulletin] HPSBUX03512 SSRT102254 rev.1 - HP-UX Web Server Suite running Apache, I
From: security-alert () hp ! com
Date: 2015-10-15 16:59:10
Message-ID: 20151015165910.36529205B0 () 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.hpe.com/portal/site/hpsc/public/kb/
docDisplay?docId=emr_na-c04832246

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04832246
Version: 1

HPSBUX03512 SSRT102254 rev.1 - HP-UX Web Server Suite running Apache, 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: 2015-10-15
Last Updated: 2015-10-15

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

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP-UX Web Server
Suite running Apache. These vulnerabilities could be exploited remotely to
create a Denial of Service (DoS) and other impacts including...

  - The TLS vulnerability using US export-grade 512-bit keys in
Diffie-Hellman key exchange known as "Logjam" could be exploited remotely to
allow unauthorized modification.
  - The RC4 stream cipher vulnerability in SSL/TLS known as "Bar Mitzvah"
could be exploited remotely to allow disclosure of information.

References:

CVE-2013-5704
CVE-2014-0118
CVE-2014-0226
CVE-2014-0231
CVE-2015-3183
CVE-2015-4000 - "Logjam"
CVE-2015-2808 - "Bar Mitzvah"
SSRT102254

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX Web Server Suite 2.2.15.21 Apache

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2013-5704	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2014-0118	(AV:N/AC:M/Au:N/C:N/I:N/A:P)	4.3
CVE-2014-0226	(AV:N/AC:M/Au:N/C:P/I:P/A:P)	6.8
CVE-2014-0231	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	5.0
CVE-2015-3183	(AV:N/AC:L/Au:N/C:N/I:P/A:N)	5.0
CVE-2015-4000	(AV:N/AC:M/Au:N/C:N/I:P/A:N)	4.3
CVE-2015-2808	(AV:N/AC:M/Au:N/C:P/I:N/A:N)	4.3

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

RESOLUTION

HP has provided the following software updates to resolve the vulnerabilities

with HP-UX Web Server Suite running Apache.

The updates are available for download from http://software.hp.com

NOTE: HP-UX Web Server Suite v3.31 HPUXWSATW331 contains the following components:

- Apache v2.2.15.23
- Tomcat Servlet Engine 5.5.36.02
- PHP 5.2.17.04

HP-UX 11i Release
Apache Depot name

B.11.23 (11i v2 32-bit)
HP_UX_11.23_HP_UX_11.23_HPUXWS22ATW-B331-11-23-32.depot

B.11.23 (11i v2 64-bit)
HP_UX_11.23_HP_UX_11.23_HPUXWS22ATW-B331-11-23-64.depot

MANUAL ACTIONS: Yes - Update
Download and install the software 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 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
=============
hpuxws22APACHE32.APACHE
hpuxws22APACHE32.APACHE2
hpuxws22APACHE32.AUTH_LDAP
hpuxws22APACHE32.AUTH_LDAP2
hpuxws22APACHE32.MOD_JK
hpuxws22APACHE32.MOD_JK2
hpuxws22APACHE32.MOD_PERL
hpuxws22APACHE32.MOD_PERL2
hpuxws22APACHE32.PHP
hpuxws22APACHE32.PHP2
hpuxws22APACHE32.WEBPROXY
hpuxws22APACHE32.WEBPROXY2
hpuxws22APACHE.APACHE
hpuxws22APACHE.APACHE2
hpuxws22APACHE.AUTH_LDAP
hpuxws22APACHE.AUTH_LDAP2
hpuxws22APACHE.MOD_JK
hpuxws22APACHE.MOD_JK2
hpuxws22APACHE.MOD_PERL
hpuxws22APACHE.MOD_PERL2
hpuxws22APACHE.PHP
hpuxws22APACHE.PHP2
hpuxws22APACHE.WEBPROXY
hpuxws22APACHE.WEBPROXY2
action: install revision B.2.2.15.18 or subsequent

hpuxws22TOMCAT32.TOMCAT
hpuxws22TOMCAT.TOMCAT
action: install revision C.6.0.35.01 or subsequent

END AFFECTED VERSIONS

HISTORY
Version:1 (rev.1) - 15 October 2015 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

Copyright 2015 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 v2.0.19 (GNU/Linux)

iEYEARECAAYFAlYfx08ACgkQ4B86/C0qfVnAPgCcD1TArWUoxWzLfCuWwOFStft/
ykwAoLdFUZfsjmnzKg/Tg7sUg3pCdD0m
=ickD
-----END PGP SIGNATURE-----

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

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