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

List: bugtraq
Subject: [security bulletin] HPSBUX03363 rev.1 - HP-UX Apache Web Server running OpenSSL, Remote Di
From: security-alert () hp ! com
Date: 2015-07-08 16:57:42
Message-ID: 20150708165742.2AC21201DE () 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-c04725401

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04725401
Version: 1

HPSBUX03363 rev.1 - HP-UX Apache Web Server running OpenSSL, Remote
Disclosure of Information

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

Release Date: 2015-07-08
Last Updated: 2015-07-08

Potential Security Impact: Remote disclosure of information

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

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with OpenSSL which may
impact HP-UX Apache Web Server with SSL/TLS enabled.

This is the TLS vulnerability using US export-grade 512-bit keys in
Diffie-Hellman key exchange known as "Logjam" which could be exploited
remotely resulting in disclosure of information.

Note: The default configuration of HP-UX Apache Web Server is not vulnerable.

References:

  CVE-2015-4000 (SSRT102106)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX Apache Web Server - all versions if both EDH and EXPORT ciphers are
enabled.

BACKGROUND

CVSS 2.0 Base Metrics
===
  Reference   Base Vector   Base Score
CVE-2015-4000   (AV:N/AC:M/Au:N/C:N/I:P/A:N)   4.3
===
             Information on CVSS is documented
            in HP Customer Notice: HPSN-2008-002

RESOLUTION

HP has provided the following workaround to resolve the vulnerability in
HP-UX Apache Web Server.

  Note: The HP-UX Apache Web Server with default configuration is not
vulnerable because the default configuration does not support the DH ciphers.

  Since the HP-UX Apache Web Server might be vulnerable if both EDH and
EXPORT ciphers have been enabled, run the following commands to check:

    # openssl s_client -connect <server_name>:443 -cipher "EDH"

    # openssl s_client -connect <server_name>:443 -cipher "EXP"

  If both connections succeed, then the following workaround should be
applied.

Workaround:

Change the following Apache configuration settings to disable the vulnerable DH and EXPORT ciphers:

Example from the default configuration file:

1. Edit the Apache SSL configuration file: "httpd-ssl.conf".

2. Change "+EXP" to "!EXP" or append ":!EXP" if not in the list:

SSLCipherSuite !ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:!EXP:+eNULL

3. Restart the Apache Web Server.

HISTORY
Version:1 (rev.1) - 8 July 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

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.19 (GNU/Linux)

iEYEARECAAYFAlWdUNUACgkQ4B86/C0qfVlHVwCg5o9ztoYCH37tfJAjzjWEqakn 59QAoNcuE+YdZnybEwxsZgYf8GLoe6uf
=7Aeq
-----END PGP SIGNATURE-----

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

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