

[[prev in list](#)] [[next in list](#)] [[prev in thread](#)] [[next in thread](#)]

List: [bugtraq](#)
Subject: [security bulletin] HPSBUX03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Information
From: [security-alert\(.\)hp!com](#)
Date: [2015-08-05 18:16:19](#)
Message-ID: [20150805181619.8939920B10\(.\)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-c04760669

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04760669
Version: 1

HPSBUX03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Information

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

Release Date: 2015-08-05
Last Updated: 2015-08-05

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 HP-UX running OpenSSL 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.

References:

- CVE-2015-4000: DHE man-in-the-middle protection (Logjam).
 - CVE-2015-1788: Malformed ECParameters causes infinite loop.
 - CVE-2015-1789: Exploitable out-of-bounds read in X509_cmp_time.
 - CVE-2015-1790: PKCS7 crash with missing EnvelopedContent
 - CVE-2015-1791: Race condition handling NewSessionTicket
 - CVE-2015-1792: CMS verify infinite loop with unknown hash function
 - CVE-2015-1793: Alternative Chain Certificate Forgery.
- SSRT102180

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.31 running OpenSSL 1.0.1m or earlier.

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
CVE-2015-1788     (AV:N/AC:M/Au:N/C:N/I:N/A:P)  4.3
CVE-2015-1789     (AV:N/AC:M/Au:N/C:N/I:N/A:P)  4.3
CVE-2015-1790     (AV:N/AC:L/Au:N/C:N/I:N/A:P)  5.0
CVE-2015-1791     (AV:N/AC:M/Au:N/C:P/I:P/A:P)  6.8
CVE-2015-1792     (AV:N/AC:L/Au:N/C:N/I:N/A:P)  5.0
CVE-2015-1793     (AV:N/AC:L/Au:N/C:P/I:P/A:N)  6.4
=====

```

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

RESOLUTION

HP has provided an updated version of OpenSSL to resolve this vulnerability.

A new B.11.31 depot for OpenSSL_A.01.00.01p is available here:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=OPENSSL11I>

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 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.11.31

=====

openssl.OPENSSL-CER

openssl.OPENSSL-CONF

openssl.OPENSSL-DOC

openssl.OPENSSL-INC

openssl.OPENSSL-LIB

openssl.OPENSSL-MAN

openssl.OPENSSL-MIS

openssl.OPENSSL-PRNG

openssl.OPENSSL-PVT

openssl.OPENSSL-RUN

openssl.OPENSSL-SRC

action: install revision A.01.00.01p or subsequent

END AFFECTED VERSIONS

HISTORY

Version:1 (rev.1) - 5 August 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

6/26/26, 7:31 PM '[security bulletin] HPSBUX03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Infor' - MARC
other countries. Other product and company names mentioned herein may be
trademarks of their respective owners.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.11 (GNU/Linux)

iEYEARECAAYFA1XCSD4ACgkQ4B86/C0qfV1KnQCg5XcK1amrTACEyDY3QtJF75u2
L90AnAgGXxSCZgBVzDQCAezbHbrHPwtg
=74KM

-----END PGP SIGNATURE-----

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)