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

List: bugtraq
Subject: [security bulletin] HPSBGN03351 rev.1 - HP IceWall SSO Dfw, SSO Certd, MCRP, and Federatio
From: security-alert () hp ! com
Date: 2015-06-26 17:41:09
Message-ID: 20150626174109.F3A7520624 () 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-c04710027

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04710027
Version: 1

HPSBGN03351 rev.1 - HP IceWall SSO Dfw, SSO Certd, MCRP, and Federation Agent
running OpenSSL, Remote Disclosure of Information

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

Release Date: 2015-06-26
Last Updated: 2015-06-26

Potential Security Impact: Remote disclosure of information, unauthorized
access

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

VULNERABILITY SUMMARY
Potential security vulnerabilities have been identified with HP IceWall SSO
Dfw, SSO Certd, MCRP, and Federation Agent running OpenSSL. This is the TLS
vulnerability known as "Logjam", which could be exploited remotely to allow
disclosure of information.

References:

CVE-2015-4000
SSRT102103

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP IceWall MCRP v3.0
HP IceWall SSO Dfw v10.0
HP IceWall SSO Certd v10.0
HP IceWall Federation Agent v3.0

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 recommends the following software updates and workaround instructions to
resolve the vulnerabilities for HP IceWall SSO Dfw, SSO Certd, MCRP, and
Federation Agent.

1. IceWall SSO Dfw v10.0 and Certd v10.0, which are running on RHEL, could
be using either the OS bundled OpenSSL library or the OpenSSL bundled with HP
IceWall. If still using the OpenSSL bundled with HP IceWall, please switch to
the OpenSSL library bundled with the OS, and then follow the instructions in
step 2.

Documents are available at the following location with instructions to
switch to the OS bundled OpenSSL library:

http://www.hp.com/jp/icewall_patchaccess

2. For HP IceWall products running on RHEL and are using the OS bundled OpenSSL, RHEL has provided a patch, for RHEL6 only, at the following location:

https://rhn.redhat.com/errata/RHSA-2015-1072.html

3. For IceWall products running on HP-UX which are using the OS bundled OpenSSL, please follow the WORKAROUND INSTRUCTIONS.

WORKAROUND INSTRUCTIONS

HP recommends the following information to protect against potential risk from CVE-2015-4000 for the following HP IceWall products.

HP IceWall SSO Dfw and MCRP

- If possible, do not use the SHOST setting which allows IceWall SSO Dfw or MCRP to use SSL/TLS protocol to back-end web servers.

- If possible, do not use EXPORT-grade ciphers on the back-end web servers.

HP IceWall SSO Certd

- If possible, do not use the LDAPSSL setting which allows IceWall SSO Certd to connect to the LDAP server using SSL/TLS protocol.

- If possible, do not use EXPORT-grade ciphers on the LDAP server.

IceWall Federation Agent

- If possible, use "bindings:HTTP-POST" instead of "bindings:HTTP-Artifact" setting in the service provider meta file. The "bindings:HTTP-POST" setting would disable IWFA to use SSL for communicating with IdP server.

Note: The HP IceWall product is only available in Japan.

HISTORY
Version:1 (rev.1) - 26 June 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

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)

iEYEARECAAYFAlWNjqkACgkQ4B86/C0qfVndPQCgv5pcAv5bmO0n2TOXMPqRdWOm
mI0AnRQo6aP+pNX1v8i7H8/7iGRw8yHy
=2FR8
-----END PGP SIGNATURE-----

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

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