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

List: bugtraq
Subject: [security bulletin] HPSBGN03373 rev.1 - HP Release Control running TLS, Remote Disclosure
From: security-alert () hp ! com
Date: 2015-07-10 17:35:44
Message-ID: 20150710173544.1C924207FC () 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-c04740527

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04740527
Version: 1

HPSBGN03373 rev.1 - HP Release Control running TLS, Remote Disclosure of
Information

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

Release Date: 2015-07-10
Last Updated: 2015-07-10

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 Release
Control running TLS.

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 (SSRT102132)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Release Control v9.13, v9.20, v9.21, v9.21P1, and v9.21P2

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 information at the following location to resolve the
vulnerability in HP Release Control:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsea
rch/document/KM01708694

HISTORY
Version:1 (rev.1) - 10 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)

iEYEARECAAYFAlWf+cgACgkQ4B86/C0qfVkhGACg+kLPIZt3BTd4g11SFXV7WsJ6
cgcAoPZyGgPGfJC8rB7vsSmd9JegQ1Xk
=KXIw
-----END PGP SIGNATURE-----

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

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