

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

List: [bugtraq](#)  
Subject: [security bulletin] HPSBGN03405 rev.1 - HP Integration Adaptor, Remote Unauthorized Modification  
From: [security-alert\(.\)hp!com](#)  
Date: [2015-08-26 14:54:19](#)  
Message-ID: [20150826145419.54C3D21819\(.\)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-c04773004](https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04773004)

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04773004  
Version: 1

HPSBGN03405 rev.1 - HP Integration Adaptor, Remote Unauthorized Modification, Disclosure of Information

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

Release Date: 2015-08-25  
Last Updated: 2015-08-25

Potential Security Impact: Remote unauthorized modification, disclosure of information

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

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified in HP Integration Adaptor.

- 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-2015-4000 - "Logjam"  
CVE-2015-2808 - "Bar Mitzvah"  
SSRT102214

SUPPORTED SOFTWARE VERSIONS\*: ONLY impacted versions are listed.  
HP Integration Adaptor v9.12.

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-2015-2808	(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 made the following mitigation information available to resolve the vulnerability for the impacted versions of HP Integration Adaptor.

Please consult HP Software Support Online (SSO):

[https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01763510?lang=en&cc=us&hpappid=113963\\_OSP\\_PRO\\_HPE](https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01763510?lang=en&cc=us&hpappid=113963_OSP_PRO_HPE)

HISTORY

Version:1 (rev.1) - 25 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

**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](mailto:security-alert@hp.com).

**Report:** To report a potential security vulnerability with any HP supported product, send Email to: [security-alert@hp.com](mailto: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](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)

iEYEARECAAYFA1XcmY4ACgkQ4B86/C0qfVmj7wCfTQBQT74m2enq5IIrb9II5+do  
9m8AoIqsy5s0D9ABNrEnGv/cwa81598Q  
=w09x

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

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

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