

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

List: [bugtraq](#)
Subject: [security bulletin] HPSBMU03356 rev.1 - HP Business Service Automation Essentials (BSAE) r
From: [security-alert\(.\)hp!com](#)
Date: [2015-06-22 18:48:24](#)
Message-ID: [20150622184824.0A21E207BB\(.\)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-c04718196

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04718196
Version: 1

HPSBMU03356 rev.1 - HP Business Service Automation Essentials (BSAE) running TLS, Remote Disclosure of Information

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

Release Date: 2015-06-22
Last Updated: 2015-06-22

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 Business Service Automation Essentials (BSAE) 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 (SSRT102112)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Business Service Automation Essentials (BSAE) v9.10, v9.11, and v9.20

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 Business Service Automation Essentials (BSAE):

<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facets/search/document/KM01660793>

HISTORY

Version:1 (rev.1) - 22 June 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=hpsecbulletins

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)

iEYEARECAAYFA1WISjEACgkQ4B86/C0qfVn/SQCfQu0YBSUHWJQB+BZMwMaoxg7w
/ooAn1Rvp/f1/YV0Q4007Ns51LGw1yRf
=9D4C

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

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

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