

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

List: [bugtraq](#)
Subject: [security bulletin] HPSBGN03533 rev.1 - HP Enterprise Cloud Service Automation and Codar, I
From: [security-alert\(.\)_hpe ! com](#)
Date: [2016-01-29 18:21:36](#)
Message-ID: [20160129182136.76C5A10BA4A\(.\)_psrt ! rose ! rdlabs ! hpecorp ! net](#)
[Download RAW [message](#) or [body](#)]

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

UPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04953655
Version: 1

HPSBGN03533 rev.1 - HP Enterprise Cloud Service Automation and Codar, Remote Unauthorized Modification

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

Release Date: 2016-01-29
Last Updated: 2016-01-29

Potential Security Impact: Remote Unauthorized Modification

Source: Hewlett Packard Enterprise, Product Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability in the TLS protocol was addressed by the HPE Cloud Service Automation and Codar products. This vulnerability known as "Logjam" could be exploited remotely to allow unauthorized modification.

References: CVE-2015-4000

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HPE Cloud Service Automation CSA 3.2, CSA 4.0, CSA 4.01, CSA 4.10 and CSA 4.2
HPE CODAR CODAR 1.0

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

Hewlett Packard Enterprise has provided the following instructions to fix this vulnerability in Cloud Service Automation and Codar:

Disable the cipher suite related to Diffie-Hellman in Cloud Service Automation and CODAR using the instructions provided at the following links:

KB link for Cloud Service Automation:

<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01855113>

KB link for CODAR:

<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01855415>

HISTORY

Version:1 (rev.1) - 29 January 2016 Initial release

Third Party Security Patches: Third party security patches that are to be installed on systems running Hewlett Packard Enterprise (HPE) 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 HPE Services support channel. For other issues about

Report: To report a potential security vulnerability with any HPE supported product, send Email to: security-alert@hpe.com

Subscribe: To initiate a subscription to receive future HPE Security Bulletin alerts via Email: <http://www.hpe.com/support/Subscriber Choice>

Security Bulletin Archive: A list of recently released Security Bulletins is available here: <http://www.hpe.com/support/Security Bulletin Archive>

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 = HPE General Software
HF = HPE Hardware and Firmware
MU = Multi-Platform Software
NS = NonStop Servers
OV = OpenVMS
PV = ProCurve
ST = Storage Software
UX = HP-UX

Copyright 2016 Hewlett Packard Enterprise

Hewlett Packard Enterprise 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 Enterprise and the names of Hewlett Packard Enterprise products referenced herein are trademarks of Hewlett Packard Enterprise 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 v1

iQEcBAEBAgAGBQJWq5fZAAoJEGIGBBYqR09/lqMIAM06ogsUy1Wat2DAYXWh3gVu
XhbWSU0Sk02b1gxzjwdk3q/xYx300MnGX0oVR7395PI8JEKnyuDkCl2STKVGEJJB
b1n2+IVowddm8I+rRghKevjzaIlbiZv1Rr32tnG8WTC90sxooctNV+xpRhBuzgw2
X15U8t9eWaatGnWznkft5E2qwMyk81N1WzFJ144sWQwaaAyH9mE5hKjvBoc4gZj1
RSSLdxu5tQoRTuU2vOYwa2k2bLcJ9oA22oH9QD5d62aWINFFu1T8GGpdWepE+N2J
qSBdji1FRKxd7HqEIpFq5a0Ea0gx05W26y2JzCpM8WHAddhI69+P2YuT2TwAQGA=
=4C0H

-----END PGP SIGNATURE-----
[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

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