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

List: bugtraq
Subject: [security bulletin] HPSBMU03401 rev.1 - HP Operations Manager for UNIX and Linux, Remote U
From: security-alert () hp ! com
Date: 2015-08-31 16:46:31
Message-ID: 20150831164631.CD3CC20353 () 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.hpe.com/portal/site/hpsc/public/kb/
docDisplay?docId=emr_na-c04770140

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c04770140
Version: 1

HPSBMU03401 rev.1 - HP Operations Manager for UNIX and Linux, Remote
Unauthorized Modification, Disclosure of Information

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

Release Date: 2015-08-31
Last Updated: 2015-08-31

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 Operations
Manager for UNIX and Linux.

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"
SSRT102212

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP Operations Manager for UNIX and Linux v9.10, v9.11, v9.20, and v9.21

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 update available for HP Operations Manager for UNIX
and Linux to resolve the vulnerabilities. Please consult HP Software Support
Online (SSO):

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsea
rch/document/KM01777542?lang=en&cc=us&hpappid=113963_OSP_PRO_HPE

HISTORY
Version:1 (rev.1) - 31 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
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 v1.4.11 (GNU/Linux)

iEYEARECAAYFAlXkgh4ACgkQ4B86/C0qfVlElACg2UuzUcejFm4liH0prGLN/Brz
vpYAoPocUhPllOebDrd9kI09cRWfOdA3
=MPoU
-----END PGP SIGNATURE-----
[prev in list] [next in list] [prev in thread] [next in thread]

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