

SSRT5938 rev.0 – HP–UX perl local unauthorized elevated privileges

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2005-06/0124.html>

From: Security Alert (*secure_at_hpchs.cup.hp.com*)

Date: 06/16/05

Date: Thu, 16 Jun 2005 17:36:01 GMT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

HP SECURITY BULLETIN

HPSBUX01208 REVISION: 0

SSRT5938 rev.0 – HP–UX perl local unauthorized elevated privileges

NOTICE:

There are no restrictions for distribution of this Security Bulletin provided that it remains complete and intact.

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

INITIAL RELEASE:

15 June 2005

POTENTIAL SECURITY IMPACT:

local unauthorized elevated privileges

SOURCE:

Hewlett–Packard Company
HP Software Security Response Team

VULNERABILITY SUMMARY:

A potential security vulnerability has been identified with HP–UX running perl where the potential vulnerability could be exploited by a local user to gain unauthorized elevated privileges.

REFERENCES:

CAN–2005–0448

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP–UX B.11.00, B.11.11, and B.11.23 running perl.

BACKGROUND:

CAN–2005–0448 <<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN–2005–0448>> reports a race condition in the rmtree function in Perl prior to 5.8.4 which allows local users to create arbitrary setuid binaries in the tree being deleted.

The changes made to address this issue in Perl 5.8.4 have been incorporated into the HP–UX perl revisions cited below.

AFFECTED VERSIONS

Note: To determine if a system has an affected version, search the output of "swlist –a revision –l fileset" for an affected fileset. Then determine if the recommended patch or update is installed.

For perl version 5.8.0 and prior

HP–UX B.11.00

HP–UX B.11.11

HP–UX B.11.23

=====

Perl5.PERL–RUN

action: install revision D.5.8.0.G or subsequent

For perl 5.8.2

HP–UX B.11.00

HP–UX B.11.11

=====

Perl5.PERL–RUN,revision=D.5.8.2.A

Perl5.PERL–RUN,revision=D.5.8.2.B

Perl5.PERL–RUN,revision=D.5.8.2.C

action: install revision D.5.8.2.D or subsequent

For perl 5.8.2

HP–UX B.11.23

=====

Perl5.PERL–RUN,revision=D.5.8.2.A

Perl5.PERL–RUN,revision=D.5.8.2.B

Perl5.PERL–RUN,revision=D.5.8.2.C

Perl5.PERL–RUN,revision=D.5.8.2.D

Perl5.PERL–RUN,revision=D.5.8.2.E

action: install revision D.5.8.2.F or subsequent

For perl 5.8.3

HP–UX B.11.00

HP–UX B.11.11

HP–UX B.11.23

=====

Perl5.PERL–RUN,revision=D.5.8.3.A

comp.security.misc: SSRT5938 rev.0 – HP–UX perl local unauthorized elevated privileges

action: install revision D.5.8.3.B or subsequent

END AFFECTED VERSIONS

RESOLUTION:

HP has made the following available on <http://software.hp.com/> to resolve the issue.

PERL version 5.8.0

=====

HP–UX 11.00 PA–RISC version 5.8.0

perl_D.5.8.0.G_HP–UX_B.11.00_32+64.depot or subsequent

HP–UX 11i v1.0 PA–RISC version 5.8.0

perl_D.5.8.0.G_HP–UX_B.11.11_32+64.depot or subsequent

HP–UX 11i v1.0409 version 5.8.0 (IA and PA)

perl_D.5.8.0.G_HP–UX_B.11.23_IA+PA.depot or subsequent

PERL version 5.8.2

=====

HP–UX 11.00 PA–RISC version 5.8.2

perl_D.5.8.2.D_HP–UX_B.11.00_32+64.depot or subsequent

HP–UX 11i v1.0 PA–RISC version 5.8.2

perl_D.5.8.2.D_HP–UX_B.11.11_32+64.depot or subsequent

HP–UX 11i v1.0409 version 5.8.2 (IA and PA)

perl_D.5.8.2.F_HP–UX_B.11.23_IA+PA.depot or subsequent

PERL version 5.8.3

=====

HP–UX 11.00 PA–RISC version 5.8.3

perl_D.5.8.3.B_HP–UX_B.11.00_32+64.depot or subsequent

HP–UX 11i v1.0 PA–RISC version 5.8.3

perl_D.5.8.3.B_HP–UX_B.11.11_32+64.depot or subsequent

HP–UX 11i v1.0409 version 5.8.3 (IA and PA)

perl_D.5.8.3.B_HP–UX_B.11.23_IA+PA.depot or subsequent

MANUAL ACTIONS: Yes – Update

Updated versions of perl are available on

<http://software.hp.com/>.

BULLETIN REVISION HISTORY:

Revision 0: 15 June 2005

Initial release

HP–UX SPECIFIC SECURITY BULLETINS*: Security Patch Check revision B.02.00 analyzes all HP–issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific

HP–UX system.

For more information:

http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

SUPPORT: For further information, contact normal HP Services support channel.

REPORT: To report a potential security vulnerability with any HP supported product, send Email to: security-alert@hp.com. It is strongly recommended that security related information being communicated to HP be encrypted using PGP, especially exploit information. To obtain the security-alert PGP key please send an e-mail message to security-alert@hp.com with the Subject of 'get key' (no quotes).

SUBSCRIBE: To initiate a subscription to receive future HP Security Bulletins via Email:

http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in_SC-GEN__driverITRC&topiccode=ITRC

On the web page: ITRC security bulletins and patch sign-up
Under Step1: your IRTC security bulletins and patches
– check ALL categories for which alerts are required and continue.

Under Step2: your IRTC operating systems
– verify your operating system selections are checked and save.

To update an existing subscription:

<http://h30046.www3.hp.com/subSignIn.php>

Log in on the web page

Subscriber's choice for Business: sign-in.

On the Web page:

Subscriber's Choice: your profile summary

– use Edit Profile to update appropriate sections.

To review previously published Security Bulletins visit:

<http://itrc.hp.com/service/cki/secBullArchive.do>

* The Software Product Category that this Security Bulletin relates to is represented by the 5th and 6th characters of the Bulletin number:

GN = HP General SW,
MA = HP Management Agents,
MI = Misc. 3rd party SW,
MP = HP MPE/iX,
NS = HP NonStop Servers,

OV = HP OpenVMS,
PI = HP Printing & Imaging,
ST = HP Storage SW,
TL = HP Trusted Linux,
TU = HP Tru64 UNIX,
UX = HP–UX,
VV = HP Virtual Vault

System management and security procedures must be reviewed frequently to maintain system integrity. HP is continually reviewing and enhancing the security features of software products to provide customers with current secure solutions.

"HP is broadly distributing this Security Bulletin in order to bring to the attention of users of the affected HP products the important security information contained in this Bulletin. HP recommends that all users determine the applicability of this information to their individual situations and take appropriate action. HP does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, HP will not be responsible for any damages resulting from user's use or disregard of the information provided in this Bulletin. To the extent permitted by law, HP disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose, title and non–infringement."

(c)Copyright 2005 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 nor 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: PGP 8.1

iQA/AwUBQrFfyeAfOvwtKn1ZEQIj7wCdFkLykKtXAN8GpIM5H+4D2WwNa4kAoO/c
5p0nYAKyVQSE+Ift/aoxzd9u
=OtP8

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

--

comp.security.misc: SSRT5938 rev.0 – HP–UX perl local unauthorized elevated privileges

Yours truly,
HP S/W Security Team
WTEC Cupertino, California
Return-Path: secure@cup.hp.com
Reply-to: security-alert@hp.com