

[security bulletin] HPSBTU02322 SSRT080011 rev.1 – HP Tru64 UNIX running SSH/SFTP Server, Remote Execution of Arbitrary Code or Denial of Service (DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00336.html>

- *From:* security-alert@xxxxxx
 - *Date:* Wed, 26 Mar 2008 05:28:25 -0700
-

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

Hash: SHA1

SUPPORT COMMUNICATION – SECURITY BULLETIN

Document ID: c01404118

Version: 1

HPSBTU02322 SSRT080011 rev.1 – HP Tru64 UNIX running SSH/SFTP Server, Remote Execution of Arbitrary Code or Denial of Service (DoS)

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

Release Date: 2008-03-19

Last Updated: 2008-03-25

Potential Security Impact: Remote execution of arbitrary code or Denial of Service (DoS)

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

VULNERABILITY SUMMARY

A potential security vulnerability has been identified in the SFTP Server (sftp-server) component of SSH v 3.2.0 and earlier running on HP Tru64 UNIX. The vulnerability could be exploited by a remote user to execute arbitrary code or cause a Denial of Service (DoS).

References: CVE-2006-0705

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

The following supported software versions are affected:

SSH v 3.2.0 and earlier as provided with...

HP Tru64 UNIX v 5.1B-4

HP Tru64 UNIX v 5.1B-3

BACKGROUND

CVSS 2.0 Base Metrics

Reference Base Vector Base Score

CVE-2006-0705 (AV:N/AC:L/Au:S/C:P/I:P/A:P) 6.5

Information on CVSS is documented in HP Customer Notice: HPSN-2008-002.

RESOLUTION

HP is releasing the following Early Release Patch (ERP) kits publicly for use by any customer until updates are available in mainstream release patch kits.

The resolutions contained in the ERP kits are targeted for availability in the following mainstream kit:

HP Tru64 UNIX v 5.1B-5

The ERP kits use dupatch to install and will not install over any Customer Specific Patches (CSPs) that have file intersections with the ERPs. Contact your service provider for assistance if the installation of the ERPs is blocked by any of your installed CSPs.

The ERP kits distribute the following items:

Patched version of SSH v 3.2.0

HP Tru64 UNIX Version v 5.1B-4

PREREQUISITE: HP Tru64 UNIX v 5.1B-4 PK6 (BL27)

Name: T64KIT1001460-V51BB27-ES-20080310

Location:

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001460-V51BB27-ES-20080310>

HP Tru64 UNIX Version v 5.1B-3

PREREQUISITE: HP Tru64 UNIX v 5.1B-3 PK5 (BL26)

Name: T64KIT1001467-V51BB26-ES-20080314

Location:

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001467-V51BB26-ES-20080314>

MD5 checksums are available from the ITRC patch database main page. From the patch database main page, click Tru64 UNIX, then click verifying MD5 checksums under useful links.

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) – 25 March 2008 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

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@xxxxxx

It is strongly recommended that security related information being communicated to HP be encrypted using PGP, especially exploit information.

To get the security-alert PGP key, please send an e-mail message as follows:

To: security-alert@xxxxxx

Subject: get key

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_dri

On the web page: ITRC security bulletins and patch sign-up

Under Step1: your ITRC security bulletins and patches

– check ALL categories for which alerts are required and continue.

Under Step2: your ITRC 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://www.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 in the title:

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 VirtualVault

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."

©Copyright 2008 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: PGP 8.1

iQA/AwUBR+IHCuAfOvwtKn1ZEQKCjwCg2ndafb+g178IUWclqABGCFdrE7cAmwRU
nTAIb6xOCKIYZ/TrcgjLfiWq
=/q+4

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