

# SSRT4717 rev.0 Remote denial of service in Apache HTTP Server

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-05/0519.html>

---

*From:* Security Alert (*secure\_at\_cup.hp.com*)

*Date:* 05/17/04

Date: Mon, 17 May 2004 14:28:20 GMT

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

Hash: SHA1

HP SECURITY BULLETIN

HPSBUX01022 REVISION: 0

SSRT4717 rev.0 Remote denial of service in Apache HTTP Server

---

NOTICE:

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

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

INITIAL RELEASE: 25 April 2004

POTENTIAL SECURITY IMPACT: Remote denial of service

SOURCE: HEWLETT-PACKARD COMPANY

HP Software Security Response Team

REFERENCES: CAN-2003-0020, CAN-2004-0113, CAN-2004-0174

VULNERABILITY SUMMARY:

1. Apache does not filter terminal escape sequences from error logs, which could make it easier for attackers to insert those sequences into terminal emulators. More details are available at <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020>
2. Starvation issue on listening sockets occurs when a short-lived connection on a rarely-accessed listening socket will cause a

child to hold the accept mutex and block out new connections.

More details are available at

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174>

3. Memory leak in mod\_ssl allows a remote denial of service attack against a SSL-enabled server by sending plain HTTP requests to the SSL port. More details are available at

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0113>

SUPPORTED SOFTWARE VERSIONS\*: ONLY impacted versions are listed.

HP9000 Servers running HP-UX release B.11.00, B.11.11, B.11.22 and B.11.23 with versions of the following products are affected, and represented as: product-name, version (product-tag/bundle-tag)

- - hp apache-based web server, 2.0.43.04 or earlier (HPApache/B9416AA) This product includes Apache 2.0.43.
- - hp-ux apache-based web server, v.2.01 or earlier (hpuxwsAPACHE/hpuxwsApache) This product includes Apache 2.0.48.
- - hp apache-based web server (with IPv6 support), 2.0.43.04 or earlier (HPApache/B9416BA) This product includes Apache 2.0.43.
- - hp-ux apache-based web server(with IPv6 support), v.2.01 or earlier (hpuxwsAPACHE/hpuxwsApache) This product includes Apache 2.0.48.

#### BACKGROUND:

The Common Vulnerabilities and Exposures project has identified potential vulnerabilities in the Apache HTTP Server (CAN-2003-0020, CAN-2004-0174, and CAN-2004-0113). It affects the following HP product numbers/versions:

- - hp apache-based web server, 2.0.43.04 or earlier (HPApache/B9416AA)
- - hp-ux apache-based web server, v.2.01 or earlier (hpuxwsAPACHE/hpuxwsApache)
- - hp apache-based web server, 2.0.43.04 (with IPv6 support) or earlier (HPApache/B9416BA)
- - hp-ux apache-based web server (with IPv6 support), v.2.01 or earlier (hpuxwsAPACHE/hpuxwsApache)

#### AFFECTED VERSIONS

The following is a list of affected filesets or patches and fix information. To determine if a system has an affected version,

search the output of "swlist -a revision -l fileset" for an affected fileset or patch, then determine if a fixed revision or applicable patch is installed.

HP-UX B.11.00

HP-UX B.11.11

HP-UX B.11.22

HP-UX B.11.23

=====

HPApache.APACHE2

hpuxwsAPACHE.APACHE2

action: install hp-ux apache-based web server, v.2.03 or later

#### RESOLUTION:

The Apache Software Foundation has released Apache 2.0.49 as the best known version that fixes the problems identified in the above mentioned issues. For customers using HPApache/B9416AA HPApache/B9416BA and hpuxwsAPACHE/hpuxwsApache, HP has incorporated Apache 2.0.49 in the following product:

-- hp-ux apache-based web server v.2.03 or later

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE)

Support ended for HP-UX Web Server Suite for HP-UX 11i v1.6 (11.22) after March 31, 2004. Starting from this release HP-UX Web Server Suite for HP-UX 11i v1.6 (11.22) is no longer available or supported. Users of HP-UX Web Server Suite on HP-UX 11i v1.6 are encouraged to update to HP-UX 11i v2 (11.23) and install the latest HP-UX Web Server Suite for HP-UX 11i v2.

For HP-UX releases B.11.00, B.11.11, and B.11.23 download new HP Apache product from : <http://www.software.hp.com/>

For HPApache/B9416AA, HPApache/B9416BA and hpuxwsAPACHE/hpuxwsApache download the following:

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE)

-- hp-ux apache-based web server(with IPv6 support), v.2.03 or later (hpuxwsAPACHE/hpuxwsApache). This product includes

Apache 2.0.49.

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE)

-- hp-ux apache-based web server (with IPv4) v.2.03 or later (hpuxwsAPACHE/hpuxwsApache). This product includes Apache 2.0.49.

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE)

-- hp-ux apache-based web server(with IPv6 support), v.2.03 or later (hpuxwsAPACHE/hpuxwsApache). This product includes Apache 2.0.49.

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE)

For HP-UX release B.11.22

-- Starting from this release HP-UX Web Server Suite for HP-UX 11i v1.6 (11.22) is no longer available or supported.

Users of HP-UX Web Server Suite on HP-UX 11i v1.6 are encouraged to update to HP-UX 11i v2 (11.23) and install the latest HP-UX Web Server Suite for HP-UX 11i v2.

Check for Apache Installation

-----

To determine if the Apache web server from HP is installed on your system, use Software Distributor's swlist command. All three versions products may co-exist on a single system. For example, the results of the command

```
swlist -l product | grep -i apache
```

```
HPApache 2.0.39.01.02 HP Apache-based Web Server
```

```
hpuxwsAPACHE A.2.01 HP-UX Apache-based Web Server
```

Stop Apache

-----

Before updating, make sure to stop any previous Apache binary. Otherwise, the previous binary will continue running, preventing the new one from starting, although the installation would be successful. After determining which Apache is installed, stop

Apache with the following commands:

for HPAPache: /opt/hpapache2/bin/apachectl stop

for hpuxwsAPACHE: /opt/hpws/apache[32]/bin/apachectl stop

### Download and Install Apache

---

- - Download Apache from Software Depot using the previously mentioned links.
- - Verify successful download by comparing the cksum with the value specified on the installation web page.
- - Use SD to swinstall the depot.
- - For customers with HPAPache/B9416BA installed, migrate to hpuxwsAPACHE/hpuxwsApache and remove the affected products from the system. Installation of this new version of HP Apache over an existing HP Apache installation is supported, while installation over a non-HP Apache is NOT supported.

### Removing Apache Installation

---

If you rather remove Apache from your system than install a newer version to resolve the security problem, use both Software Distributor's "swremove" command and also "rm -rf" the home location as specified in the rc.config.d file "HOME" variables. To find the files containing HOME variables in the /etc/rc.config.d directory:

```
%ls /etc/rc.config.d | grep apache
```

```
hpapache2conf
```

```
hpws_apache[32]conf
```

MANUAL ACTIONS: Yes - Update

Install the product containing the fix. For customers with HPAPache/B9416AA HPAPache/B9416BA installed, the fix requires migration to hpuxwsAPACHE/hpuxwsApache and removing the affected products from the system.

\* The software product category that this Security Bulletin relates to is represented by the 5th and 6th characters of the Bulletin number: GN=General, MA=Management Agents, MI=Misc.

## comp.security.misc: SSRT4717 rev.0 Remote denial of service in Apache HTTP Server

3rd party, MP=HP-MPE/iX, NS=HP NonStop Servers, OV=HP OpenVMS,  
PI=HP Printing & Imaging, ST=HP Storage, TU=HP Tru64 UNIX,  
TL=Trusted Linux, UX=HP-UX, VV=Virtual Vault

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

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

On the web page:

Driver and Support Alerts/Notifications Sign-up: Product Selection

Under Step1: your products

1. Select product category:
  - a minimum of servers must be selected.
2. Select product family or search:
  - a minimum of one product must be selected.
3. Add a product:
  - a minimum of one product must be added.

In Step 2: your operating system(s)

- check ALL operating systems for which alerts are required.

Complete the form 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.

Note: In addition to the individual alerts/notifications for the selected operating systems/products, subscribers will automatically receive one copy of alerts for non-operating system categories (i.e., a subscriber who signs up for all six operating system alerts will only receive one copy of all the non-operating system alerts).

### HP-UX SPECIFIC SECURITY BULLETINS\*:

To review previously published Security Bulletins for HP-UX:

<http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin>

The HP-UX Security Patch Matrix is available here:

<http://itrc.hp.com/service/cki/docDisplay.do?docId=hpuxSecurityMatrix>

Or via anonymous ftp:

[ftp://ftp.itrc.hp.com/export/patches/hp-ux\\_patch\\_matrix/](ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix/)

The HP-UX Security Patch Matrix, updated daily, categorizes security patches by platform/OS release, and by Bulletin topic.

The Security Patch Check tool completely automates the process of reviewing the Security Patch Matrix for HP-UX 11.XX Versions.

NOTE: Installing patches listed in the Security Patch Matrix will completely implement the RESOLUTION in the Security Bulletin \_only\_ if there are no MANUAL ACTIONS included.

The Security Patch Check tool can also verify that a Security Bulletin RESOLUTION has been implemented on HP-UX 11.XX Versions provided that no MANUAL ACTIONS were included. The Security Patch Check tool cannot verify patches implemented via product upgrade.

For information on the Security Patch Check tool, see:

[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA)

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).

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 2004 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

comp.security.misc: SSRT4717 rev.0 Remote denial of service in Apache HTTP Server

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 8.0.2

iQA/AwUBQKUUzeAfOvwtKn1ZEQKCKgCfTH1u0NQ1mRVmjshNU6ie0m/sbtUAn1CP  
ORTY/dANWjtaSrDC3OdDVmI8  
=taPy

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

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