

# SSRT3622 rev.0 HP-UX remote denial of service using AAA Server

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-05/0515.html>

---

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

**Date:** 05/17/04

Date: Mon, 17 May 2004 14:24:34 GMT

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

Hash: SHA1

HP SECURITY BULLETIN

HPSBUX01011 REVISION: 0

SSRT3622 rev.0 HP-UX remote denial of service using AAA 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: 8 April 2004

LAST UPDATED: 8 April 2004

POTENTIAL SECURITY IMPACT: Remote denial of service

SOURCE: HEWLETT-PACKARD COMPANY

HP Software Security Response Team

REFERENCES: CAN-2004-0079, CAN-2004-0112, CAN-2004-0081,  
CERT TA04-078A

VULNERABILITY SUMMARY:

A potential security vulnerability has been identified with  
the HP-UX AAA server where an unauthenticated remote attacker  
could cause a denial of service.

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

comp.security.misc: SSRT3622 rev.0 HP-UX remote denial of service using AAA Server

HP-UX B.11.00, and B.11.11 running HP-UX AAA Server A.06.01.02.04 or earlier.

HP-UX B.11.23 running HP-UX AAA Server A.06.01.02.06.

BACKGROUND:

The HP-UX AAA Server uses components of the OpenSSL functions internally and is therefore vulnerable to the following items.

CAN-2004-0079: Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool uncovered a null-pointer assignment in the do\_change\_cipher\_spec() function. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. Depending on the application this could lead to a denial of service. All versions of OpenSSL from 0.9.6c to 0.9.6k inclusive and from 0.9.7a to 0.9.7c inclusive are affected by this issue.

CAN-2004-0112: Stephen Henson discovered a flaw in SSL/TLS handshaking code when using Kerberos ciphersuites. A remote attacker could perform a carefully crafted SSL/TLS handshake against a server configured to use Kerberos ciphersuites in such a way as to cause OpenSSL to crash. Most applications have no ability to use Kerberos ciphersuites and will therefore be unaffected. Versions 0.9.7a, 0.9.7b, and 0.9.7c of OpenSSL are affected by this issue.

CAN-2004-0081: Testing performed by the OpenSSL group using the Codenomicon TLS Test Tool uncovered a bug in older versions of OpenSSL 0.9.6 that can lead to a Denial of Service attack (infinite loop). This issue was traced this to a fix that was added to OpenSSL 0.9.6d some time ago.

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.

HP-UX B.11.23  
HP-UX B.11.11  
HP-UX B.11.00

=====

AAAServer  
action: install revision A.06.01.02.07 or subsequent.

END AFFECTED VERSIONS

RESOLUTION:

SSRT3622 rev.0 HP-UX remote denial of service using AAA Server

comp.security.misc: SSRT3622 rev.0 HP–UX remote denial of service using AAA Server

For HP–UX releases B.11.00, B.11.11, and B.11.23, download a new HP–UX AAA Server product A.06.01.02.07 or later from

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1428AA>

in order to completely resolve these issues. This product includes OpenSSL 0.9.7c + patch.

Please write to [security-alert@hp.com](mailto:security-alert@hp.com) to request a PGP signed version of this bulletin.

MANUAL ACTIONS: Yes – Update

Go to

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1428AA>

to download a current version of the HP–UX AAA Server software.

\* 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. 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=VirtualVault

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](mailto:security-alert@hp.com)

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 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 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

iQA/AwUBQHXRpuAfOvwtKn1ZEQIwfQCg7VxLuRpp2E97ZQI0tM6U30q7yoYAnj2I  
Iq3YbtZQRR6xJbapzSZ3l0Pm  
=0EUg

-----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