

FreeBSD Security Advisory

FreeBSD-SA-04:05.openssl

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-03/0103.html>

From: FreeBSD Security Advisories (security-advisories_at_freebsd.org)

Date: 03/17/04

Date: Wed, 17 Mar 2004 08:48:32 -0800 (PST)

To: FreeBSD Security Advisories <security-advisories@freebsd.org>

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

Hash: SHA1

=====

FreeBSD-SA-04:05.openssl Security Advisory
The FreeBSD Project

Topic: Denial-of-service vulnerability in OpenSSL

Category: crypto

Module: openssl

Announced: 2004-03-17

Credits: OpenSSL Project <[URL:http://www.openssl.org](http://www.openssl.org)>

Codenomicon Ltd <[URL:http://www.codenomicon.com](http://www.codenomicon.com)>

Affects: All FreeBSD 4.x and 5.x releases

Corrected: 2004-03-17 12:23:51 UTC (RELENG_4, 4.9-STABLE)

2004-03-17 12:14:12 UTC (RELENG_5_2, 5.2.1-RELEASE-p3)

2004-03-17 12:14:56 UTC (RELENG_5_1, 5.1-RELEASE-p16)

2004-03-17 12:17:13 UTC (RELENG_4_9, 4.9-RELEASE-p4)

2004-03-17 12:18:23 UTC (RELENG_4_8, 4.8-RELEASE-p17)

CVE Name: CAN-2004-0079

FreeBSD only: NO

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit

<[URL:http://www.freebsd.org/security/](http://www.freebsd.org/security/)>.

I. Background

FreeBSD includes software from the OpenSSL Project. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography

library.

II. Problem Description

When processing an SSL/TLS ChangeCipherSpec message, OpenSSL may fail to check that a new cipher has been previously negotiated. This may result in a null pointer dereference.

III. Impact

A remote attacker could perform a specially crafted SSL/TLS handshake with an application that utilizes OpenSSL, triggering the null pointer dereference and causing the application to crash. Depending upon the specifics of the application, this may result in an effective denial-of-service.

IV. Workaround

No workaround is known.

V. Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4–STABLE; or to the RELENG_5_2, RELENG_4_9, or RELENG_4_8 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.8, 4.9, 5.1, and 5.2 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:05/openssl.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:05/openssl.patch.asc
```

b) Execute the following commands as root:

```
# cd /usr/src  
# patch < /path/to/patch
```

c) Recompile the operating system as described in
<URL: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/makeworld.html >.

Note that any statically linked applications that are not part of the base system (i.e. from the Ports Collection or other 3rd-party sources) must be recompiled.

All affected applications must be restarted for them to use the corrected library. Though not required, rebooting may be the easiest way to accomplish this.

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

Branch Revision
Path

RELENG_4

src/crypto/openssl/crypto/opensslv.h 1.1.1.1.2.9
src/crypto/openssl/ssl/s3_pkt.c 1.1.1.1.2.7

RELENG_5_2

src/UPDATING 1.282.2.11
src/crypto/openssl/crypto/opensslv.h 1.1.1.14.2.1
src/crypto/openssl/ssl/s3_pkt.c 1.1.1.8.4.1
src/sys/conf/newvers.sh 1.56.2.10

RELENG_5_1

src/UPDATING 1.251.2.18
src/crypto/openssl/crypto/opensslv.h 1.1.1.13.2.1
src/crypto/openssl/ssl/s3_pkt.c 1.1.1.8.2.1
src/sys/conf/newvers.sh 1.50.2.18

RELENG_4_9

src/UPDATING 1.73.2.89.2.5
src/crypto/openssl/crypto/opensslv.h 1.1.1.1.2.8.2.1
src/crypto/openssl/ssl/s3_pkt.c 1.1.1.1.2.6.4.1
src/sys/conf/newvers.sh 1.44.2.32.2.5

RELENG_4_8

src/UPDATING 1.73.2.80.2.20
src/crypto/openssl/crypto/opensslv.h 1.1.1.1.2.7.2.1
src/crypto/openssl/ssl/s3_pkt.c 1.1.1.1.2.6.2.1
src/sys/conf/newvers.sh 1.44.2.29.2.18

VII. References

<URL: http://www.openssl.org/news/secadv_20040317.txt >

<URL: <http://cvs.openssl.org/chngview?cn=12033> >

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (FreeBSD)

iD8DBQFAWH8nFdaIBMps37IRAgSZAkCPXaoTb16c8JGJL+Uz7eOX8/864ACbB059

AIfN8fbeiGJ3fdG0pKAMwMw=

=2f24

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

freebsd–security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd–security>

FreeBSD–Security: FreeBSD Security Advisory FreeBSD–SA–04:05.openssl

To unsubscribe, send any mail to "freebsd–security–unsubscribe@freebsd.org"