CERT Advisory CA-2002-23 Multiple Vulnerabilities In OpenSSL

Original release date: July 30, 2002
Last revised: October 11, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- OpenSSL prior to 0.9.6e, up to and including pre-release 0.9.7-beta2
- OpenSSL pre-release 0.9.7-beta2 and prior with Kerberos enabled
- SSLeay library

Overview

There are four remotely exploitable buffer overflows in OpenSSL. There are also encoding problems in the ASN.1 library used by OpenSSL. Several of these vulnerabilities could be used by a remote attacker to execute arbitrary code on the target system. All could be used to create denial of service.

I. Description

OpenSSL is a widely deployed, open source implementation of the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The SSL and TLS protocols are used to provide a secure connection between a client and a server for higher level protocols such as HTTP. Four remotely exploitable vulnerabilities exist in many OpenSSL client and server systems.

VU#102795 - OpenSSL servers contain a buffer overflow during the SSLv2 handshake process

> *Versions of OpenSSL servers prior to 0.9.6e and pre-release version 0.9.7-beta2 contain a remotely exploitable buffer overflow vulnerability. This vulnerability can be exploited by a client using a malformed key during the handshake process with an SSL server connection. Note that only SSLv2-supported sessions are affected by this issue.*
>
> *This issue is also being referenced as CAN-2002-0656.*

VU#258555 - OpenSSL clients contain a buffer overflow during the SSLv3 handshake process

> *OpenSSL clients using SSLv3 prior to version 0.9.6e and pre-release version 0.9.7-beta2 contain a buffer overflow vulnerability. A malicious server can exploit this by sending a large session ID to the client during the handshake process.*
>
> *This issue is also being referenced as CAN-2002-0656.*

VU#561275 - OpenSSL servers with Kerberos enabled contain a remotely exploitable buffer overflow vulnerability during the SSLv3 handshake process

> *Servers running OpenSSL pre-release version 0.9.7 with Kerberos enabled contain a remotely exploitable buffer overflow vulnerability. This vulnerability can be exploited by a malicious client sending a malformed key during the SSLv3 handshake process with the server.*
>
> *This issue is also being referenced as CAN-2002-0657.*

VU#308891 - OpenSSL contains multiple buffer overflows in buffers that are used to hold ASCII representations of integers

> *OpenSSL clients and servers prior to version 0.9.6e and pre-release version 0.9.7-beta2 contain multiple remotely exploitable buffer overflow vulnerabilities if running on 64-bit platforms. These buffers are used to hold ASCII representations of integers.*
>
> *This issue is also being referenced as CAN-2002-0655.*

In addition, a separate issue has been identified in OpenSSL involving malformed ASN.1 encodings. Affected components include SSL or TLS applications, as well as S/MIME, PKCS#7, and certificate creation routines.

VU#748355 - ASN.1 encoding errors exist in implementations of SSL, TLS, S/MIME, PKCS#7 routines

> *The ASN.1 library used by OpenSSL has various encoding errors that allow malformed certificate encodings to be parsed incorrectly. Exploitation of this vulnerability can lead to remote denial-of-service issues. Routines affected include those supporting SSL and TLS applications, as well as those supporting S/MIME, PKCS#7, and certificate creation.*
>
> *This issue is also being referenced as CAN-2002-0659.*

Although these vulnerabilities affect OpenSSL, other implementations of the SSL protocol that use or share a common code base may be affected. This includes implementations that are derived from the SSLeay library developed by Eric A. Young and Tim J. Hudson.

As noted in the OpenSSL advisory as well, sites running OpenSSL 0.9.6d servers on 32-bit platforms with SSLv2 handshaking disabled will not be affected by any of the buffer overflows described above. However, due to the nature of the ASN.1 encoding errors, such sites may still be affected by denial-of-service situations.

II. Impact

By exploiting the buffer overflows above, a remote attacker can execute arbitrary code on a vulnerable server or client system or cause a denial-of-service situation. Exploitation of the ASN.1 encoding errors can lead to a denial of service.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments. Please contact your vendor directly.

Upgrade to version 0.9.6e of OpenSSL

Upgrade to version 0.9.6e of OpenSSL to resolve the issues addressed in this advisory. As noted in the OpenSSL advisory, separate patches are available:

> *Combined patches for OpenSSL 0.9.6d:*
> *http://www.openssl.org/news/patch_20020730_0_9_6d.txt*

After either applying the patches above or upgrading to 0.9.6e, recompile all applications using OpenSSL to support SSL or TLS services, and restart said services or systems. This will eliminate all known vulnerable code.

Sites running OpenSSL pre-release version 0.9.7-beta2 may wish to upgrade to 0.9.7-beta3, which corrects these vulnerabilities. Separate patches are available as well:

> *Combined patches for OpenSSL 0.9.7 beta 2:*
> *http://www.openssl.org/news/patch_20020730_0_9_7.txt*

Disable vulnerable applications or services

Until fixes for these vulnerabilities can be applied, disable all applications that use vulnerable implementations of OpenSSL. Systems with OpenSSL 0.9.7 pre-release with Kerberos enabled also need to disable Kerberos to protect against VU#561275. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. Before deciding to disable SSL or TLS, carefully consider the impact that this will have on your service requirements.

Disabling SSLv2 handshaking will prevent exploitation of VU#102795. However, due to the nature of the ASN.1 encoding errors, such sites would still be vulnerable to denial-of-service attacks.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments.

Apple Computer, Inc.

> *The vulnerabilities described in this note are fixed with Security Update 2002-08-02.*

Alcatel

>

> *In relation to this CERT advisory on security vulnerability in OpenSSL, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that various Alcatel products are affected: namely the 6600, 7700, 7800 and 8800 OmniSwitches, the OmniAccess 210 and the 7770 RCP. Alcatel is currently in the process of applying appropriate fixes to those products. Customers may contact their Alcatel support representative for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential security vulnerabilities in our products using OpenSSL and will provide updates if necessary.*

Covalent Technologies

> *Covalent Technologies has been informed by RSA Security that the BSAFE libraries used in Covalent's SSL implementations are potentially vulnerable to the SSL V2 negotiation issue detailed in VU#102795 and the related CA-2002-23 and CA-2002-27 advisories. All Covalent products using SSL are affected. Covalent has product updates and additional information available at:*
>
> > *http://www.covalent.net/products/rotate.php?page=110*

Debian Project

> *The Debian project has released DSA 136 a while ago which fixes this vulnerability. Here's the link:*
>
> > *http://www.debian.org/security/2002/dsa-136*

IBM

> *IBM's AIX operating system does not ship with OpenSSL; however, OpenSSL is available for installation on AIX via the Linux Affinity Toolkit. The version included on the Toolkit CD is vulnerable to the issues discussed here as will as the version of OpenSSL available for downloading from the IBM Linux Affinity website. Anyone running this version is advised to upgrade to the new version available from the website. This will be available within the next few days and can be downloaded from*
>
> > *http://www6.software.ibm.com/dl/aixtbx/aixtbx-p*
>
> *This site contains Linux Affinity applications using cryptographic algorithms. New users to this site are asked to register first.*

ISC

> *ISC Vendor statement.*
>
> *BIND 4, BIND 8 and BIND 9.0.x are not vulnerable.*
>
> *BIND 9.1.x ship with a copy of the vulnerable sections of OpenSSL crypto library (obj_dat.c and asn1_lib.c). Please upgrade to BIND 9.2.x and/or relink with a fixed version OpenSSL. e.g. configure --with-openssl=/path/to/fixed/openssl Vendors shipping product based on BIND 9.1 should contact bind-bugs@isc.org.*
>
> *BIND 9.2.x is vulnerable if linked against a vulnerable library. By default BIND 9.2 does not link against OpenSSL.*

Juniper Networks

> *Juniper has determined that our JUNOS Internet software (on M- and T-series routers) and the software running on our SDX and SSC products are potentially susceptible to the security vulnerabilities in OpenSSL. Corrected software images will be available for customer download shortly.*
>
> *Software for our G10 CMTS product and our ERX products is unaffected by these vulnerabilities.*

Lotus Software

> *Lotus products do not use OpenSSL or an SSLeay library, so they are not vulnerable. We further analyzed our SSL implementation for the issues reported in the advisory and determined that our products are not vulnerable.*

Mandrake Software

> *Mandrake Linux update advisory MDKSA-2002:046-1 fixes all of these issues in OpenSSL. Please see*
>
> > *http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-046-1.php*

Microsoft Corporation

> *Microsoft products do not use the libraries in question. Microsoft products are not affected by this issue.*

NetBSD

> *Please see NetBSD-SA2002-009*

OpenLDAP

> *The OpenLDAP Project uses OpenSSL. Rebuilding OpenLDAP with updated versions of OpenSSL should adequately address reported issues. Those using packaged versions of OpenLDAP should contact the package distributor for update information.*

OpenSSL

> *Please see http://www.openssl.org/news/secadv_20020730.txt.*

Red Hat

> *Red Hat distributes affected versions of OpenSSL in all Red Hat Linux distributions as well as the Stronghold web server. Red Hat Linux errata packages that fix the above vulnerabilities (CAN-2002-0655 and CAN-2002-0656) are available from the URL below. Users of the Red Hat Network are able to update their systems using the 'up2date' tool. A future update will fix the potential remote DOS in the ASN.1 encoding (CAN-2002-0659)*
>
> > *http://rhn.redhat.com/errata/RHSA-2002-155.html*

Secure Computing Corporation

> *In response to the CERT Advisory CA-2002-23, Secure Computing has posted a software patch for all users of the SafeWord PremierAccess version 3.1 authentication system. All existing and new customers are advised to download and apply PremierAccess Patch 1. Patch 1(3.1.0.01) is available for immediate web download at*
>
> > *http://www.securecomputing.com/index.cfm?skey=1109*

These vulnerabilities were discovered and reported by the following:

- VU#102795 - discovered by A.L. Digital Ltd and independently discovered and reported by John McDonald of Neohapsis
- VU#258555, VU#561275, VU#308891 - discovered by A.L. Digital Ltd
- VU#748355 - discovered by Adi Stav and James Yonan independently

The CERT/CC thanks the OpenSSL team for the work they put into their advisory, on which this document is largely based.

Feedback can be directed to the authors: Jason A. Rafail, Cory F. Cohen, Jeffrey S. Havrilla, Shawn V. Hernan.

Revision History

```
July 30, 2002: Initial release
Aug 02, 2002: Added IBM statement from 07/31/2002
Aug 07, 2002: Added NetBSD statement from 08/01/2002
Aug 07, 2002: Added Apple statement from 08/02/2002
Aug 07, 2002: Added Lotus statement from 08/02/2002
Aug 07, 2002: Added ISC statement from 07/31/2002
Aug 15, 2002: Added Juniper statement from 08/15/2002
Sep 17, 2002: Added Covalent statement from 09/16/2002
Sep 20, 2002: Added Alcatel statement from 09/03/2002
Sep 23, 2002: Added Mandrake Software statement from 09/19/2002
Sep 26, 2002: Added Microsoft Corporation statement from 09/25/2002
Sep 30, 2002: Added Secure Computing Corporation statement from 09/24/2002
Oct 11, 2002: Added Debian statement from 10/08/2002
```