CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL /TLS Implementations

Original issue date: October 1, 2003
Last revised: October 23, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- OpenSSL versions prior to 0.9.7c and 0.9.6k
- Multiple SSL/TLS implementations
- SSLeay library

Overview

There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service.

I. Description

SSL and TLS are used to provide authentication, encryption, and integrity services to higher-level network applications such as HTTP. Cryptographic elements used by the protocols, such as X.509 certificates, are represented as ASN.1 objects. In order to encode and decode these objects, many SSL and TLS implementations (and cryptographic libraries) include ASN.1 parsers.

OpenSSL is a widely deployed open source implementation of the SSL and TLS protocols. OpenSSL also provides a general-purpose cryptographic library that includes an ASN.1 parser.

The U.K. National Infrastructure Security Co-ordination Centre (NISCC) has developed a test suite to analyze the way SSL and TLS implementations handle exceptional ASN.1 objects contained in client and server certificate messages. Although the test suite focuses on certificate messages, any untrusted ASN.1 element may be used as an attack vector. An advisory from OpenSSL describes as vulnerable "Any application that makes use of OpenSSL's ASN1 library to parse untrusted data. This includes all SSL or TLS applications, those using S/MIME (PKCS#7) or certificate generation routines."

There are two certificate message attack vectors. An attacker can send crafted client certificate messages to a server, or attempt to cause a client to connect to a server under the attacker's control. When the client connects, the attacker can deliver a crafted server certificate message. Note that the standards for TLS (RFC 2246) and SSL 3.0 state that a client certificate message "...is only sent if the server requests a certificate." To reduce exposure to these types of attacks, an SSL/TLS server should ignore unsolicited client certificate messages (VU#732952).

NISCC has published two advisories describing vulnerabilities in OpenSSL (006489/OpenSSL) and other SSL/TLS implementations (006489/TLS). The second advisory covers multiple vulnerabilities in many vendors' products. Further details, including vendor status information, are available in the following vulnerability notes.

VU#935264 - OpenSSL ASN.1 parser insecure memory deallocation
A vulnerability in the way OpenSSL deallocates memory used to store ASN.1 structures could allow a remote attacker to execute arbitrary code with the privileges of the process using the OpenSSL library.
(Other resources: NISCC/006490/OpenSSL/3, OpenSSL #1, CAN-2003-0545)

VU#255484 - OpenSSL contains integer overflow handling ASN.1 tags (1)
An integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.
(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0543)

VU#380864 - OpenSSL contains integer overflow handling ASN.1 tags (2)
A second integer overflow vulnerability in the way OpenSSL handles ASN.1 tags could allow a remote attacker to cause a denial of service.
(Other resources: NISCC/006489/OpenSSL/1, OpenSSL #2, CAN-2003-0544)

VU#686224 - OpenSSL does not securely handle invalid public key when configured to ignore errors
A vulnerability in the way OpenSSL handles invalid public keys in client certificate messages could allow a remote attacker to cause a denial of service. This vulnerability requires as a precondition that an application is configured to ignore public key decoding errors, which is not typically the case on production systems.
(Other resources: NISCC/006489/OpenSSL/2, OpenSSL #3)

VU#732952 - OpenSSL accepts unsolicited client certificate messages
OpenSSL accepts unsolicited client certificate messages. This could allow an attacker to exploit underlying flaws in client certificate handling, such as the vulnerabilities listed above.
(Other resources: OpenSSL #4)

VU#104280 - Multiple vulnerabilities in SSL/TLS implementations
Multiple vulnerabilities exist in different vendors' SSL/TLS implementations. The impacts of these vulnerabilities include remote execution of arbitrary code, denial of service, and disclosure of sensitive information. VU#104280 covers an undefined set of vulnerabilities that affect SSL/TLS implementations from many different vendors. The other vulnerabilities listed above are specific to OpenSSL.
(Other resources: NISCC/006489/TLS)

II. Impact

The impacts of these vulnerabilities vary. In almost all, a remote attacker could cause a denial of service. For at least one vulnerability in OpenSSL (VU#935264), a remote attacker may be able to execute arbitrary code. Please see Appendix A, the Systems Affected section of VU#104280, and the OpenSSL vulnerability notes for details.

III. Solution

Upgrade or apply a patch

To resolve the OpenSSL vulnerabilities, upgrade to OpenSSL 0.9.7c or OpenSSL 0.9.6k. Alternatively, upgrade or apply a patch as directed by your vendor. Recompile any applications that are statically linked to OpenSSL libraries.

For solutions for the other SSL/TLS vulnerabilities covered by VU#104280, please see Appendix A and the Systems Affected section of VU#104280.

Appendix A. Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated, and the changes are noted in the revision history. If a vendor is not listed below, we have not received their authenticated, direct statement. Further vendor information is available in the Systems Affected sections of the vulnerability notes listed above.

AppGate Network Security AB

> *The default configuration of AppGate is not vulnerable. However some extra functionality which administrators can enable manually may cause the system to become vulnerable. For more details check the AppGate support pages at http://www.appgate.com/support .*

Apple Computer Inc.

> *Apple: Vulnerable. This is fixed in Mac OS X 10.2.8 which is available from http://www.apple.com/support/*

Check Point

> *Check Point products are vulnerable to: VU#732952 09/04/2003 OpenSSL accepts unsolicited client certificate messages VU#380864 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (2) VU#255484 09/30/2003 OpenSSL contains integer overflow handling ASN.1 tags (1) A fix will be released by Oct 27th 2003. Check Point products are not vulnerable to: VU#686224 09/30/2003 OpenSSL does not securely handle invalid public key when configured to ignore errors VU#935264 09/30/2003 OpenSSL ASN.1 parser insecure memory deallocation*

Clavister

> *Clavister Firewall: Not vulnerable*
>
> *As of version 8.3, Clavister Firewall implements an optional HTTP/S server for purposes of user authentication. However, since this implementation does not support client certificates and has no ASN.1 parser code, there can be no ASN.1-related vulnerabilities as far as SSL is concerned.*
>
> *Earlier versions of Clavister Firewall do not implement any SSL services.*

Cray Inc.

> *Cray Inc. supports OpenSSL through its Cray Open Software (COS) package. The OpenSSL version in COS 3.4 and earlier is vulnerable. Spr 726919 has been opened to address this.*

cryptlib

> *cryptlib does not appear to be vulnerable to the malformed ASN.1 data, either with or without the use of its internal ASN.1 firewall.*

Debian

> *Corrected OpenSSL packages are available in Debian Security Advisory 393, at http://www.debian.org/security/2003/dsa-393 [See also: DSA-394.]*

F5 Networks

> *F5 products BIG-IP, 3-DNS, ISMan and Firepass are vulnerable. F5 will have ready security patches for each of these products. Go to ask.f5.com for the appropriate security response instructions for your product.*

Hitachi

> *Hitachi is investigating the potential impact to Hitachi's software products. As further information becomes available Hitachi will provide notice of the Information.*
>
> *Hitachi Web Server is under investigation. (Since there was a non-investigated portion, it is under re-investigation.)*

IBM

> *[AIX]*
>
> *The AIX Security Team is aware of the issues discussed in CERT Vulnerability Notes VU#255484, VU#380864, VU#686224, VU#935264 and VU#732952.*
>
> *OpenSSL is available for AIX via the AIX Toolbox for Linux. Please note that the Toolbox is made available "as-is" and is unwarranted. The Toolbox ships with OpenSSL 0.9.6g which is vulnerable to the issues referenced above. A patched version of OpenSSL will be provided shortly and this vendor statement will be updated at that time.*
>
> *Please note that OpenSSH, which is made available through the Expansion Pack is not vulnerable to these issues.*
>
> *[eServer]*
>
> *IBM eServer Platform Response*
>
> *For information related to this and other published CERT Advisories that may relate to the IBM eServer Platforms (xSeries, iSeries, pSeries, and zSeries) please go to https://app-06.www.ibm.com/servers/resourcelink/lib03020.nsf/pages/securityalerts?OpenDocument&pathID=*
>
> *In order to access this information you will require a Resource Link ID. To subscribe to Resource Link go to http://app-06.www.ibm.com/servers/resourcelink and follow the steps for registration.*
>
> *All questions should be refered to servsec@us.ibm.com.*

Ingrian Networks

> *Ingrian Networks is aware of this vulnerablity and will issue a security advisory when our investigation is complete.*

Juniper Networks

> *The OpenSSL code included in domestic versions of JUNOS Internet Software that runs on all M-series and T-series routers is susceptible to these vulnerabilities. The SSL library included in Releases 2.x and 3.x of SDX provisioning software for E-series routers is susceptible to these vulnerabilities.*
>
> *Solution Implementation*
>
> *Corrections for all the above vulnerabilities are included in all versions of JUNOS built on or after October 2, 2003. Customers should contact Juniper Networks Technical Assistance Center (JTAC) for instructions on obtaining and installing the corrected code.*
>
> *SDX software built on or after October 2, 2003, contain SSL libraries with corrected code. Contact JTAC for instructions on obtaining and installing the corrected code.*

MandrakeSoft

> *The vulnerabilities referenced by VU#255484, VU#380864, and VU#935264 have been corrected by packages released in our MDK SA-2003:098 advisory.*

NEC Corporation

> *Subject: VU#104280*
>
> *sent on October 1, 2003*
>
> *[Server Products]*
>
> - *EWS/UP 48 Series operating system*
>   *- is NOT vulnerable.*
>   *It doesn't include SSL/TLS implementation.*

Nortel Networks

> *The SSL implementation of the following Nortel Networks products is based on OpenSSL and may be affected by the vulnerabilities identified in NISCC Vulnerability Advisory 006489/OpenSSL:*
>
> *Alteon Switched Firewall*
> *Alteon iSD - SSL Accelerator*
> *Contivity*
> *Succession Communication Server 2000 - Compact (CS2K - Compact)*
> *Preside Service Provisioning*
>
> *Other Nortel Networks products with SSL implementations are being reviewed and this Vendor Statement may be revised.*
>
> *For more information please contact*
>
> *North America: 1-800-4NORTEL or 1-800-466-7835*
>
> *Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009*
>
> *Contacts for other regions are available at http://www.nortelnetworks.com/help/contact/global/*
>
> *Or visit the eService portal at http://www.nortelnetworks.com/cs under Advanced Search.*
>
> *If you are a channel partner, more information can be found under http://www.nortelnetworks.com/pic under Advanced Search*

Novell

> *Novell is reviewing our application portfolio to identify products affected by the vulnerabilities reported by the NISCC. We have the patched OpenSSL code and are reviewing and testing it internally, and preparing patches for our products that are affected. We expect the first patches to become available via our Security Alerts web site (http://support.novell.com/security-alerts) during the week of 6 Oct 2003. Customers are urged to monitor our web site for patches to versions of our products that they use and apply them expeditiously.*

OpenSSL

> *Please see OpenSSL Security Advisory [30 September 2003].*

Openwall GNU/*/Linux

> *Openwall GNU/*/Linux currently uses OpenSSL 0.9.6 branch and thus was affected by the ASN.1 parsing and client certificate handling vulnerabilities pertaining to those versions of OpenSSL. It was not affected by the potentially more serious incorrect memory deallocation vulnerability (VU#935264, CVE CAN-2003-0545) that is specific to OpenSSL 0.9.7.*
>
> *Owl-current as of 2003/10/01 has been updated to OpenSSL 0.9.6k, thus correcting the vulnerabilities.*

Red Hat

> *Red Hat distributes OpenSSL 0.9.6 in various Red Hat Linux distributions and with the Stronghold secure web server. Updated packages which contain backported patches for these issues are available along with our advisories at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.*
>
> *Red Hat Enterprise Linux:*
> *http://rhn.redhat.com/errata/RHSA-2003-293.html*
>
> *Red Hat Linux 7.1, 7.2, 7.3, 8.0:*
> *http://rhn.redhat.com/errata/RHSA-2003-291.html*
>
> *Stronghold 4 cross-platform:*
> *http://rhn.redhat.com/errata/RHSA-2003-290.html*
>
> *Red Hat distributes OpenSSL 0.9.7 in Red Hat Linux 9. Updated packages which contain backported patches for these issues are available along with our advisory at the URL below. Users of the Red Hat Network can update their systems using the 'up2date' tool.*
>
> *Red Hat Linux 9:*
> *http://rhn.redhat.com/errata/RHSA-2003-292.html*

Riverstone Networks

> *Riverstone Networks routers are not vulnerable.*

RSA Security

> *The issues raised in this vulnerability report have been analysed in terms of impact on RSA BSAFE SSL-C, RSA BSAFE SSL-C Micro Edition, and RSA BSAFE Cert-C Micro Edition. None of these issues have been determined by RSA Security to be security critical, the products are either not impacted by the vulnerabilities raised or the impact is limited to additional Denial of Sevice opportunities.*
>
> *As part of RSA Security standard product support lifecycle, fixes for those vulnerabilities which are relevant for each product listed will be incorporated in the next maintenance release. RSA Security customers with current support and maintenance contracts may request a software upgrade for new product versions online at <https://www.rsasecurity.com/go/form_ins.html>.*

SCO

> *We are aware of the issue and are diligently working on a fix. [CSSA-2003-SCO.25]*

Secure Computing Corporation

> *Sidewinder(r) and Sidewinder G2 Firewall(tm) (including all appliances)*
>
> *Sidewinder v5.x and Sidewinder G2 v6.x are not vulnerable to the arbitrary code execution attacks described in this advisory. The Sidewinder's embedded Type Enforcement technology strictly limits the capabilities of each component which implements SSL. Any attempt to exploit this vulnerability in the SSL library code running on the firewall results in an automatic termination of the attacker's connection and multiple Type Enforcement alarms.*
>
> *Any component attacked by the denial of service (DOS) attacks described in this advisory is automatically restarted by the firewall's watchdog process without interuption of any active connections. However, under some circumstances this DOS could cause a delay in managing the firewall.*
>
> *To mitigate this inconvenience, customers should contact Secure Computing Customer Support.*
>
> *Gauntlet(tm) & e-ppliance*
>
> *Gauntlet and e-ppliance do not include any components based on OpenSSL, and are thus immune to these vulnerabilities.*

SGI

> *SGI acknowledges receiving the vulnerabilities reported by CERT and NISCC. CAN-2003-0543 [VU#255484], CAN-2003-0544 [VU#380864] and CAN-2003-0545 [VU#935264] have been addressed by SGI Security Advisory 20030904-01-P:*
>
> *ftp://patches.sgi.com/support/free/security/advisories/20030904-01-P.asc*
>
> *No further information is available at this time.*
>
> *For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported SGI operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on http://www.sgi.com/support/security/*

Sun Microsystems Inc.

> *Sun is currently investigating Solaris 7, 8, and 9 to determine the full potential impact of these SSL/TLS vulnerabilities.*
>
> *The Solaris Secure Shell daemon, sshd(1M), shipped with Solaris 9, is not affected by these vulnerabilities.*
>
> *Java Secure Sockets Extension 1.0.x and J2SE 1.4.x are also not affected.*
>
> *Sun Linux and Sun Cobalt both ship vulnerable versions of OpenSSL, a Sun Alert has been published here:*
>
> *http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/57100*

Stonesoft

> *Stonesoft has published a security advisory that addresses the issues in vulnerability notes VU#255484 and VU#104280. The advisory is at http://www.stonesoft.com/document/art/3040.html*

Stunnel

> *Stunnel requires the OpenSSL libraries for compilation (POSIX) or OpenSSL DLLs for runtime operation (Windows). While Stunnel itself is not vulnerable, it's dependence on OpenSSL means that your installation likely is vulnerable.*
>
> *If you compile from source, you need to install a non-vulnerable version of OpenSSL and recompile Stunnel.*
>
> *If you use the compiled Windows DLLs from stunnel.org, you should download new versions which are not vulnerable. OpenSSL 0.9.7c DLLs are available at http://www.stunnel.org/download/stunnel/win32/openssl-0.9.7c/*
>
> *No new version of Stunnel source or executable will be made available, because the problems are inside OpenSSL -- Stunnel itself does not have the vulnerability.*

SuSE

> *All SuSE products are affected. Update packages are being tested and will be published on Wednesday, October 1st. [SuSE-SA: 2003:043]*

VanDyke

> *None the VanDyke Software products are subject to these vulnerabilities due to the fact that OpenSSL is not used in any VanDyke products.*

Appendix B. References

- CERT/CC Vulnerability Note VU#935264 - <http://www.kb.cert.org/vuls/id/935264>
- CERT/CC Vulnerability Note VU#255484 - <http://www.kb.cert.org/vuls/id/255484>
- CERT/CC Vulnerability Note VU#380864 - <http://www.kb.cert.org/vuls/id/380864>
- CERT/CC Vulnerability Note VU#686224 - <http://www.kb.cert.org/vuls/id/686224>
- CERT/CC Vulnerability Note VU#732952 - <http://www.kb.cert.org/vuls/id/732952>
- CERT/CC Vulnerability Note VU#104280 - <http://www.kb.cert.org/vuls/id/104280>
- OpenSSL Security Advisory [30 September 2003] - <http://www.openssl.org/news/secadv_20030930.txt>
- NISCC Vulnerability Advisory 006489/OpenSSL - <http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm>

- NISCC Vulnerability Advisory 006489/TLS - <http://www.uniras.gov.uk/vuls/2003/006489/tls.htm>
- ITU ASN.1 documentation - <http://www.itu.int/ITU-T/studygroups/com10/languages/>

NISCC discovered and researched these vulnerabilities; this document is based on their work. We would like to thank Stephen Henson of the OpenSSL project and the Oulu University Secure Programming Group (OUSPG) for their previous work in this area.

Feedback can be directed to the author, Art Manion.

Revision History

October 1, 2003: Initial release, added RSA Security statement
October 2, 2003: Updated SuSE statement
October 3, 2003: Updated SCO statement
October 8, 2003: Added Debian statement, updated Hitachi statement
October 15, 2003: Added Secure Computing statement
October 22, 2003: Added Check Point and cryptlib statements, updated RSA statement, fixed NISCC references
October 23, 2003: Updated Debian statement
October 24, 2003: Added Sun and Nortel statements