Cisco Security Advisory

Transport Layer Security Renegotiation Remote Man-in-the-Middle Attack Vulnerability

Advisory ID: Cisco-SA-20091105-CVE-2009-3555
Last Updated: 2012 August 14 16:24 GMT
Published: 2009 November 5 19:53 GMT
Version75.0: Final
CVSS Score: Base - 4.3
Workarounds: See below

CVE-2009-3555
CWE-20

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

Multiple Transport Layer Security (TLS) implementations contain a vulnerability when renegotiating a TLS session that could allow an unauthenticated, remote attacker to conduct a man-in-the-middle attack.

The vulnerability exists during a TLS renegotiation process. If an attacker can intercept traffic from a client to a TLS server, the attacker could stage a rogue TLS server to intercept that traffic and appear to authenticate the client to what the client thinks is the desired TLS server. The attacker is then able to authenticate to the legitimate TLS server and thus stage a man-in-the-middle attack. However, the attacker would not be able to view the contents of the session and would only be able to inject data or requests into it.

Proof-of-concept code that exploits this vulnerability is publicly available.

OpenSSL has confirmed this vulnerability in a changelog and released updated software.

To exploit this vulnerability, the attacker must be able to intercept traffic from a TLS client to a TLS server. In many cases, this may require the attacker to have access to a network that is adjacent to the targeted user's system. Another possibility would be for the attacker to have access to a network that is adjacent to a legitimate TLS server.

This vulnerability is likely to affect multiple implementations of TLS.

Affected Products

Apache has released a changelog at the following link: Changes with Apache 2.2.15

Apple has released security updates at the following links: Security Update 2010-001, Java for Mac OS X 10.6 Update 3, and Java for Mac OS X 10.5 Update 8

Cisco has re-released a security advisory at the following link: cisco-sa-20091109-tls. This advisory contains associated bug ID numbers; however, these numbers are likely to change as products are confirmed vulnerable or not vulnerable.

Citrix has released security advisories at the following link: CTX123359

F5 has released a security advisory for registered users at the following link: CVE-2009-3555

FreeBSD has released security advisory at the following link: FreeBSD-SA-09:15.ssl

FreeBSD has released a VuXML document at the following link: mozilla -- multiple vulnerabilities

HP has released security bulletins at the following links: c01945686 at HPSBUX02482 SSRT090249, c02079216 at HPSBUX02517 SSRT100058,c02171256 at HPSBMA02534 SSRT090180, c02122104 at HPSBUX02524 SSRT100089, c02436041 at HPSBGN02562 SSRT090249, c02512995 at HPSBMA02568 SSRT100219, c02616748 at HPSBUX02608 SSRT100333, c03263573 at HPSBMU02759 SSRT100817, and c03281831 at HPSBOV02762 SSRT100825. HP has also released security bulletins c01963123 and c02273751 for registered users at the following links: HPSBU02498 SSRT090264 and HPSBMA02547 SSRT100179

IBM has released APARs at the following links: PK96157, PM12247, and PM10658. IBM has released advisories at the following links: swg24025312, swg21415080, swg21426108, swg24006386, and swg21607116. IBM has re-released a security alert at the following link: CVE-2009-3555. IBM has released an APAR for registered users at the following link: IC68055

Microsoft has released a security bulletin, security advisory, and a knowledge base article at the following links: MS10-049, Microsoft Security Advisory (977377), and KB 977377

MontaVista Software has released a security alert for registered users on March 9, 2012, at the following link: MontaVista Security Fixes

Mozilla has released a security advisory at the following link: MFSA 2010-22

NetBSD has released a security advisory at the following link: NetBSD-SA2010-002

Novell has released a security advisory at the following link: 7005950

OpenBSD has released security announcements at the following links: 004: Security FIX: November 26, 2009 and 010: SECURITY FIX: November 26, 2009

OpenOffice.org has released a security bulletin at the following link: CVE-2009-3555

Oracle has released a security alert at the following link: Critical Patch Update March 2010

Red Hat has released security advisories at the following links: RHSA-2009:1579, RHSA-2009:1580, RHSA-2010:0011, RHSA-2010:0119, RHSA-2010:0130, RHSA-2010:0155, RHSA-2010:0162, RHSA-2010:0163, RHSA-2010:0164, RHSA-2010:0165, RHSA-2010:0166, RHSA-2010:0167, RHSA-2010:0339, RHSA-2010:0408, RHSA-2010:0440, RHSA-2010:0770, RHSA-2010:0786, RHSA-2010:0807, RHSA-2010:0986, and RHSA-2010:0987

Sun has re-released security advisories at the following links: 273029, 273350, and 274990

Sun has released a security notification at the following link: CVE-2009-3555

US-CERT has released a vulnerability note at the following link: VU#120541

VMware has released security advisories at the following links: VMSA-2010-0015 and VMSA-2010-0019

Vulnerable Products

The following implementations are vulnerable:

- OpenSSL versions prior to version 0.9.8l
- GnuTLS versions 2.8.5 and prior

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators are advised to physically secure internal networks and use switches rather than hubs to route the data.

Administrators are advised to run both firewall and antivirus applications to minimize the potential of inbound and outbound threats.

Fixed Software

OpenSSL has released updated software at the following link: openssl-0.9.8l.tar.gz

Apache has released updated software at the following link: Apache HTTP Server 2.2.15

Apple has released updated software at the following links:

Mac OS X and Mac OS X Server 10.6.4
Security Update 2010-001 (Snow Leopard)
Java for Mac OS X 10.6 Update 3

Mac OS X and Mac OS X Server 10.5.8
Security Update 2010-001 Client (Leopard)
Security Update 2010-001 Server (Leopard)
Java for Mac OS X 10.5 Update 8

CentOS packages can be updated using the **up2date** or **yum** command.

F5 has released updated software for registered users at the following link: F5 Products

FreeBSD has released patches at the following HTTP link: ssl.patch

FreeBSD releases ports collection updates at the following link: Ports Collection Index

HP has released updated software at the following links:

x86
HP System Management Homepage for Linux version 6.2

AMD64/EM64T
HP System Management Homepage for Linux version 6.2

x86/x64
HP System Management Homepage for Windows version 6.2

B.11.11 PA (32 and 64)
OpenSSL_A.00.09.08l.001
OpenSSL_A.00.09.08n.001_HP-UX_B.11.11_32+64.depot
Apache 2.0.59.13 PA-64-32-1111.depot

B.11.23 (PA and IA)
OpenSSL_A.00.09.08l.002
OpenSSL_A.00.09.08n.002_HP-UX_B.11.23_IA-PA.depot
Apache 2.0.59.13 IA-PA-32-1123.depot
Apache 2.0.59.13 IA-PA-64-1123.depot

B.11.31 (PA and IA)
OpenSSL_A.00.09.08l.003
OpenSSL_A.00.09.08n.003_HP-UX_B.11.31_IA-PA.depot
Apache 2.0.59.13 IA-PA-32-1131.depot
Apache 2.0.59.13 IA-PA-64-1131.depot

HP System Management Homepage
v6.1.0.102 or subsequent (for Windows)
v6.1.0-103 or subsequent (for Linux x86)
v6.1.0-103 or subsequent (for Linux AMD64/EM64T)

HP-UX B.11.31
JDK and JRE v6.0.07 or subsequent
JDK and JRE v5.0.20 or subsequent
SDK and JRE v1.4.2.25 or subsequent
JDK and JRE v6.0.09 or subsequent
JDK and JRE v5.0.21 or subsequent

HP-UX B.11.23
JDK and JRE v6.0.07 or subsequent
JDK and JRE v5.0.20 or subsequent
SDK and JRE v1.4.2.25 or subsequent
JDK and JRE v6.0.09 or subsequent
JDK and JRE v5.0.21 or subsequent

HP-UX B.11.11
JDK and JRE v6.0.07 or subsequent
JDK and JRE v5.0.20 or subsequent
SDK and JRE v1.4.2.25 or subsequent
JDK and JRE v6.0.09 or subsequent
JDK and JRE v5.0.21 or subsequent

HP Systems Insight Manager (SIM)
v6.1 or subsequent (for HP-UX, Linux, and Windows)

HP ProCurve Threat Management Services zl Module
Version ST.1.1.100430 or subsequent

CSWS_JAVA V3.2
HP has released updated software for registered users at the following link:

HP Onboard Administrator 3.50

IBM has released interim fixes at the following links: swg24025312 and swg24006386. IBM has released APARs at the following links: PK96157, PM12247, and PM10658. Users of the IBM JDK are advised to install JSSE APAR IZ65239. IBM has released updates at the following links: IBM developer kits, IBM DB2 version 9.1 Fix Pack 9, and IBM DB2 version 9.7 Fix Pack 2.
IBM has released a fix at the following link: IBM Tivoli Endpoint Manager 8.2.1310.

Microsoft customers can obtain updates directly by using the links in the security bulletin. These updates are also distributed by Windows automatic update features and available on the Windows Update website. Microsoft Windows Server Update Services (WSUS), Systems Management Server, and System Center Configuration Manager can assist administrators in deploying software updates.

MontaVista Software has released updated software at the following links:
PRO 5.0
Pro 5.0.24
Mobilinux 5.0.24
MVL 5
Pro 4.0.1
CGE 4.0.1
Mobilinux 4.1
Moblinux 4.0.2
CGE 5.1
Mobilinux 5.0
Mozilla has released updated software at the following links:
Firefox 3.6.2
Firefox 3.5.9
Thunderbird 3.0.4
SeaMonkey 2.0.4
NetBSD has released instructions for installing available patches at the following link: NetBSD

OpenBSD has released source code patches at the following FTP links: OpenBSD 4.5 and OpenBSD 4.6

OpenOffice.org has released an updated version at the following link: OpenOffice.org 3.2.1

Oracle has released patches for registered users at the following link: Oracle

Red Hat packages can be updated using the **up2date** or **yum** command.
Sun has released patches at the following links: **SPARC**

- Solaris 8 with patch 119209-22 or later
- Solaris 9 with patch 119211-22 or later
- Solaris 10 with patch 119213-21 or later
- Sun Java Enterprise System 5 with patch 125358-10 or later
- Sun Java System Web Server 7.0 update 7 or later
- Sun Java System Web Server 7.0 with patch 125437-18 or later
- Sun Java System Web Proxy Server 4.0.13 or later
- Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128640-15 or later (for customers with valid support contract) or 141709-03 or later (for customers without valid support contract)
- Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128643-15 or later (for customers with valid support contract) or 141700-03 or later (for customers without valid support contract)
- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later
- Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 142807-02 or later

Intel

- Solaris 9 with patch 119212-22 or later
- Solaris 10 with patch 119214-21 or later
- Sun Java Enterprise System 5 with patch 125359-10 or later
- Sun Java System Web Server 7.0 update 7 or later
- Sun Java System Web Server 7.0 with patch 125438-18 or later
- Sun Java System Web Proxy Server 4.0.13 or later
- Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128641-15 or later (for customers with valid support contract) or 141710-03 or later (for customers without valid support contract)
- Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128644-15 or later (for customers with valid support contract) or 141701-03 or later (for customers without valid support contract)
- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later
- Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 142807-02 or later

Linux

- Sun Java Enterprise System 2005Q4 and Sun Java Enterprise System 5 (for RHEL2.1 and RHEL3.0) with patch 142506-03 or later
- Sun Java Enterprise System 5 (for RHEL4.0 and RHEL5.0) with patch 121656-21 or later
- Sun Java System Web Server 7.0 update 7 or later
- Sun Java System Web Server 7.0 with patch 125439-16 or later
- Sun Java System Application Server 8.1 with patch 119171-33 or later
- Sun Java System Web Proxy Server 4.0.13 or later
- Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128642-15 or later (for customers with valid support contract) or 141711-03 or later (for customers without valid support contract)
- Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128645-15 or later (for customers with valid support contract) or 141702-03 or later (for customers without valid support contract)
- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later
- Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 142807-02 or later

HP-UX

- Sun Java Enterprise System 2005Q4 and Sun Java Enterprise System 5 with patch 124379-12 or later
- Sun Java System Web Server 7.0 update 7 or later
- Sun Java System Web Server 7.0 with patch 125440-16 or later
- Sun Java System Web Proxy Server 4.0.13 or later
- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later
- Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 142807-02 or later

Windows

- Sun Java Enterprise System 2005Q4 with patch 124392-11 or later
- Sun Java Enterprise System 5 with patch 125923-10 or later
- Sun Java System Web Server 7.0 update 7 or later
- Sun Java System Web Server 7.0 with patch 125441-18 or later
- Sun Java System Application Server 8.1 with patch 119172-33 or later
- Sun Java System Web Proxy Server 4.0.13 or later
- Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128646-15 or later (for customers with valid support contract) or 141703-03 or later (for customers without valid support contract)
- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later
- Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 142807-02 or later

AIX

- Sun Java System Directory Server 5.2 Patch 6 with patch 142806-02 or later

Sun has released patches for StarOffice/StarSuite for relevant platforms at the following link: CVE-2009-3555

VMware has released updated software at the following links:
ESX 3.5
ESX350-201012401-SG
ESX 4.0
ESX400-201009401-SG
ESX 4.1
ESX410-201010402-SG

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20091105-CVE-2009-3555

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2009-Nov-05
