Cisco Security Advisory

OpenSSL RSA Signature Forgery Vulnerability

Advisory ID: Cisco-SA-20060905-CVE-2007-5810
Last Updated: 2015 January 31 08:15 GMT
Published: 2006 September 5 17:39 GMT
Version61.0: Final
CVSS Score: Base - 6.4
Workarounds: See below

CVE-2006-4339
CVE-2007-5810

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

OpenSSL versions 0.9.7j and prior and 0.9.8b and prior contain a vulnerability that could allow an unauthenticated, remote attacker to successfully pass a forged X.509 certificate.

The vulnerability could allow an unauthenticated, remote attacker to pass a forged Public-Key Cryptography Standards (PKCS)#1 Version 1.5 signature when signed by a certain type of RSA key. An attacker could exploit the vulnerability to access certificate-protected resources.

OpenSSL confirmed the vulnerability in a security advisory and released updated versions.

This vulnerability affects PKCS #1 v1.5 signatures if the exponent of the public key is 3, which is widely used by Certificate Authorities. An attacker will likely exploit this vulnerability to forge signatures without the secret key. PKCS #1 v1.5 is often utilized within X.509 certificates; therefore, all applications that use OpenSSL to verify X.509 certificates may be vulnerable, including software that uses OpenSSL for SSL or TLS.

Affected Products

OpenSSL has released a security advisory at the following link: September 5, 2006

Apple has released security updates at the following links: Security Update 2006-007 and Java Release 6 for Mac OS X 10.4

ARKOON has released a security advisory at the following PDF link: AK-2006-04

Attachmate has released a technical note at the following link: Technical Note 2137

Avaya has released a security advisory at the following link: ASA-2006-188

Cisco has re-released a security response at the following link: Cisco-sr-20061108-openssl. This response addresses the following bug IDs:

CSCsg22734
CSCsg01963
CSCsg09619
CSCsg16571
CSCsg17943
CSCsg24311
CSCsg46092
CSCsg04397
CSCsg04386
CSCsg51110
CSCsg51304
CSCek57074
CSCsg59589
CSCsf97055
CSCsg55732
CSCsg36592
CSCsg55738
CSCsg55742
CSCsg56292
CSCsg58599
CSCsg58607
CSCsg58592
CSCsh14665

Debian has released security advisories at the following links: DSA-1173-1 and DSA-1174-1

FreeBSD has released a security advisory at the following FTP link: FreeBSD-SA-06:19

FreeBSD has released a VuXML document at the following link: openoffice.org -- multiple vulnerabilities

Gentoo has released security advisories at the following links: GLSA 200609-05 and GLSA 200610-06

Hitachi has released a security advisory at the following link: HS07-034

HP has released security bulletins at the following links: HPSBUX02165, HPSBUX02186, HPSBTU02207 and HPSBMA02250

Ingate Systems has released a software release notice at the following link: Ingate Firewall and Ingate SIParator 4.5.1

Mandriva has released security advisories at the following links: MDKSA-2006:161, MDKSA-2006:177, MDKSA-2006:178, and MDKSA-2006:207

NetBSD has released a security advisory at the following FTP link: NetBSD-SA2006-023

Novell has released a security announcement at the following link: Novell 3143224

OpenBSD has released security announcements at the following links: 016: SECURITY FIX: September 8, 2006 and 011: SECURITY FIX: September 8, 2006

OpenOffice.org has released a security advisory at the following link: CVE-2006-4339

OpenPKG has released a security advisory at the following link: OpenPKG-SA-2006.018

OpenVPN has released a security advisory at the following link: OpenVPN 2.0.x Change Log

Opera has released a security advisory at the following link: 845

Oracle has released security advisories at the following links: BEA07-169.00 and Oracle Critical Patch Update January 2007

Red Hat has released security advisories at the following links: RHSA-2006:0661, RHSA-2007:0062, RHSA-2007:0072, RHSA-2007:0073, RHSA-2008:0264, RHSA-2008:0525, and RHSA-2008:0629

SGI has released a security advisory at the following FTP link: 20060901-01-P

Slackware has released security advisories at the following links: SSA:2006-257-02 and SSA:2006-310-01

SSH Communications has released software release notes at the following links: SSH Tectia Server 5.1.1, SSH Tectia Manager 2.2.1, SSH Tectia Server for IBM z/OS 5.2.1, and SSH Tectia Client 5.1.1

Sun has re-released alert notifications at the following links: 200196, 200474, and 200610

Sun has released a security notifcation at the following link: CVE-2006-4339

SUSE has released security announcements at the following links: SUSE-SA:2006:055, SUSE-SA:2006:061, and SUSE-SA:2007:010

SUSE has released a security summary report at the following link: SUSE-SR:2006:026

Sybase has released a security advisory at the following link: 1047991

Trustix has released security advisories at the following links: TSLSA-2006-0051 and TSLSA-2006-0063

Turbolinux has released a security advisory at the following link: TLSA-2006-29

Ubuntu Linux has released a security notice at the following link: USN-339-1

Van Dyke Technologies has published changelogs at the following links: SecureCRT 5.2.2 and SecureFX 4.0.2

VMware has released knowledge base articles at the following links: 3069097 and 9986131. VMware has released a security advisory at the following link: VMSA-2008-0005

US-CERT has released a vulnerability note at the following link: VU#845620

Vulnerable Products

OpenSSL versions 0.9.7j and prior and 0.9.8b and prior are vulnerable.

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 utilize certificates as part of a two-factor authentication system.

Administrators may consider restricting access to certificate-protected resources to trusted users through the use of a VPN or other remote access technology that is not affected.

Administrators running ISC BIND using DNSSEC are advised to apply the available software updates, generate new RSA-SHA1 and RSA-MD5 keys for all old keys, and perform a key rollover to the new keys.

Fixed Software

OpenSSL has released updated versions at the following links: OpenSSL 0.9.7k and OpenSSL 0.9.8c

Apple has released updated software at the following links:

Mac OS X 10.3.9
Mac OS X Server 10.3.9
Mac OS X 10.4.8 Intel
Mac OS X 10.4.8 PPC
Mac OS X Server 10.4.8 Universal
Mac OS X Server 10.4.8 PPC
Java for Mac OS X 10.4

ARKOON has released software updates in the ARKOON Customer Space at the following link: Client Update

Attachmate has released updated patches at the following link: Attachmate

Blue Coat has released instructions for receiving updates at the following link: Blue Coat

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via e-mail at tac@cisco.com.

Debian has released updated packages at the following links: Debian (openssl) and Debian (openssl096)

FreeBSD has released a patch at the following link: openssl.patch

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

Gentoo updates can be obtained for the following packages using the **emerge** command:

dev-libs/openssl
app-emulation/emul-linux-x86-baselibs
dev-libs/nss

HP has released updates for registered users at the following links:

- PHSS_35463 Virtualvault 4.7 OWS (Apache 1.x) update
- PHSS_35460 Virtualvault 4.7 IWS update
- PHSS_35481 Virtualvault 4.7 TGP update
- PHSS_35436 Virtualvault 4.7 OWS (Apache 2.x) update
- PHSS_35462 Virtualvault 4.6 OWS update
- PHSS_35459 Virtualvault 4.6 IWS update
- PHSS_35480 Virtualvault 4.6 TGP update
- PHSS_35461 Virtualvault 4.5 OWS update
- PHSS_35458 Virtualvault 4.5 IWS update
- PHSS_35437 Webproxy server 2.1 (Apache 2.x) update
- PHSS_35111 Webproxy server 2.1 (Apache 1.x) update
- PHSS_35110 Webproxy server 2.0 update

HP has released updated packages for HP-UX IPv4 at the following links:

HP-UX B.11.00
revision A.2.0.58.01 or later

HP-UX B.11.11
revision A.2.0.58.01 or later

HP has released updated packages for HP-UX IPv6 at the following links:

HP-UX B.11.11
revision B.2.0.58.01 or later

HP-UX B.11.23
revision B.2.0.58.01 or later

HP has released Early Release Patch kits at the following links:

- HP Tru64 UNIX v 5.1B-4 - T64KIT1001167-V51BB27-ES-20070321
- HP Tru64 UNIX v 5.1B-3 - T64KIT1001163-V51BB26-ES-20070315
- HP Tru64 UNIX v 5.1A PK6 - T64KIT1001160-V51AB24-ES-20070314
- HP Tru64 UNIX v 4.0G PK4 - T64KIT1001166-V40GB22-ES-20070316
- HP Tru64 UNIX v 4.0F PK8 - DUXKIT1001165-V40FB22-ES-20070316
- Internet Express (IX) v 6.6 BIND - CPQIM360.SSL.01.tar.gz
- HP Insight Management Agents - install the BIND 9.8.2 patch located in the appropriate ERP kit

HP has released updated software at the following links:

- HP System Management Homepage for Linux (x86) 2.1.8-177
- HP System Management Homepage for Linux (AMD64/EM64T) 2.1.8-177
- HP System Management Homepage for Windows 2.1.8-179

Ingate Systems has released software updates at the following link: Ingate Firewall and Ingate SIParator 4.5.1

The Internet Systems Consortium has released updated software for BIND at the following links: BIND 9.2.6-P2 and BIND 9.3.2-P2

Mandriva can be updated automatically using **MandrivaUpdate**. Mandrake can be updated automatically using **MandrakeUpdate**.

NetBSD has released instructions for obtaining updated packages at the following FTP link: NetBSD

Novell has released updated software at the following link: Novell International Cryptographic Infrastructure (NICI) 2.7.2

OpenBSD has released source code patches at the following FTP links: OpenBSD 3.8 and OpenBSD 3.9

OpenOffice.org has released updated software at the following link: OpenOffice 3.2

OpenPKG has released updated packages at the following FTP link: OpenPKG 2.5 - openssl-0.9.8c-2.20060906

OpenVPN has released updated software at the following link: OpenVPN 2.0.8

Opera has released an updated version at the following link: Opera 9.02 or later

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

Oracle has released updated software at the following links:

WebLogic Server 9.2

- Upgrade to Maintenance Pack 1

WebLogic Server 9.1

- Install patch CR295567 using the **Smart Update** tool

WebLogic Server 9.0

- Install the 9.0 GA Combo patch associated with Bug ID CR239280
- Apply patch CR295567_900

WebLogic Server and WebLogic Express version 8.1

- Upgrade to SP6
- Apply patch CR295567_81sp6
- Place the jar for the patch in the CLASSPATH before the weblogic.jar file

WebLogic Server and WebLogic Express version 7.0

- Upgrade to SP7
- Apply patch CR295567_70sp7
- Place the jar for the patch in the CLASSPATH before the weblogic.jar file

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

Secure Computing has released an updated version. Administrators are encouraged to contact the vendor for information on obtaining the update.

SGI has released patches for registered users at the following link: Patch 10332

Slackware packages can be updated using the **upgradepkg** command.

SSH Communications has released updated software at the following link: SSH Tectia Downloads

Sun has released patches at the following links:

- JDK and JRE 5.0 Update 9 and later (for Windows, Solaris, and Linux)
- J2SE 5.0
- J2SE 1.0.3_04
- J2SE 1.4.2

SPARC

- Sun Java Enterprise System for Solaris 8 patch 119209-17 or later
- Sun Java Enterprise System for Solaris 9 with patch 119211-17 or later
- Sun Java Enterprise System for Solaris 10 with patch 119213-17 or later
- Solaris 9 with patch 113451-14 or later
- Solaris 9 SSH patches 122300-30 and 114356-14 or later
- Solaris 9 Packaging utilities patch 113713-26 or later
- Solaris 10 with patch 119213-17 or later
- Solaris 10 with patch 120011-14 or later
- Solaris 10 with patch 120011-14 or later
- Sun Java System Application Server Enterprise with patch 119169-22 or 119166-29
- Sun Java System Application Server Platform with patch 119173-22 or 119166-29
- Sun Java System Web Server 6.0 with Service Pack 11 or later
- Sun Java System Web Server 6.1 with Service Pack 7 or later
- Sun Java System Web Server 6.1 with patch 116648-20 or later
- Sun Java System Proxy Server 4.0 with Service Pack 4 or later

Intel

- Sun Java Enterprise System for Solaris 9 with patch 119212-17 or later
- Sun Java Enterprise System for Solaris 10 with patch 119214-17 or later
- Solaris 9 with patch 114435-13 or later
- Solaris 9 SSH patches 114357-13 and 122301-30 or later
- Solaris 9 Packaging utilities patch 114568-25 or later
- Solaris 10 with patch 119214-17 or later
- Solaris 10 with patch 120012-14 or later
- Solaris 10 with patch 127128-11 or later
- Sun Java System Server Enterprise with patch 119170-22 or 119167-32
- Sun Java System Server with patch 119174-22 or 119167-32
- Sun Java System Web Server 6.1 with Service Pack 7 or later
- Sun Java System Web Server 6.1 with patch 116649-21 or later
- Sun Java System Proxy Server 4.0 with Service Pack 4 or later

J2SE 5.0

- J2SE 5.0: for Solaris 9 with patch 118666-17
- J2SE 5.0: for Solaris 9 with patch 118667-17 (64bit)
- J2SE 5.0_x86: for Solaris 9 with patch 118668-17
- J2SE 5.0_x86: for Solaris 9 with patch 118669-17 (64bit)

Linux Platform

- Sun Java Enterprise System for Linux with patch 121656-17 or later
- Sun Java System Server Enterprise without patch 119171-22 or 119168-29
- Sun Java System Server Platform without patch 119175-22 or 119168-29
- Sun Java System Web Server 6.0 with Service Pack 11 or later
- Sun Java System Web Server 6.1 with Service Pack 7 or later
- Sun Java System Web Server 6.1 with patch 118202-12 or later
- Sun Java System Proxy Server 4.0 with Service Pack 4 or later

HP-UX Platform

- Sun Java Enterprise System for HP-UX with patch 124379-08 or later
- Sun Java System Web Server 6.0 with Service Pack 11 or later
- Sun Java System Web Server 6.1 with Service Pack 7 or later
- Sun Java System Proxy Server 4.0 with Service Pack 4 or later
- Sun Java System Application Server Enterprise Edition 8.1 2005 Q1 without patch 119172-22
- Sun Java System Application Server Platform Edition 8.1 2005 Q1 without patch 119176-22
- Sun Java System Web Server 6.0 with Service Pack 11 or later
- Sun Java System Web Server 6.1 with Service Pack 7 or later
- Sun Java System Proxy Server 4.0 with Service Pack 4 or later

AIX Platform

- Sun Java System Web Server 6.0 with Service Pack 11 or later
- Sun Java System Web Server 6.1 with Service Pack 7 or later

Sun has released patches for StarOffice/StarSuite for relevant platforms at the following link: CVE-2006-4339

SUSE has released updated packages; users can install the updates using **YaST**.

Trustix products can be updated using the **swup --upgrade** command.

Turbolinux packages can be updated using the **turbopkg** command.

Ubuntu has released updated packages; users can install the updates using **Update Manager**.

Van Dyke Technologies has released updated software at the following links:

SecureCRT 5.2.2
SecureFX 4.0.2

VMware has released patches at the following links:

VMware ESX Server 3.0.1
VMware ESX Server 3.0.0
VMware ESX Server 2.5.4
VMware ESX Server 2.5.3
VMware ESX Server 2.1.3
VMware ESX Server 2.0.2

VMware has released updated versions at the following links:

VMware ACE 1.0.5
VMware ACE 2.0.1 or later
VMware Player 1.0.6
VMware Player 2.0.3
VMware Workstation 5.5.6
VMware Workstation 6.0.3
VMware Server 1.0.5

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-20060905-CVE-2007-5810

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2006-Sep-05

Legal Disclaimer