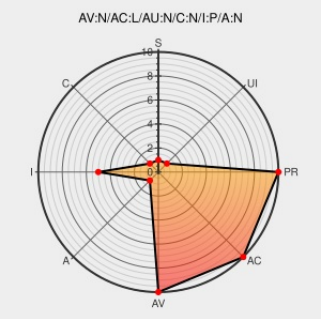
CVE-2005-2969

Published on: 10/18/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:14:31 AM UTC

CVE-2005-2969

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssl from Openssl contain the following vulnerability:

The SSL/TLS server implementation in OpenSSL 0.9.7 before 0.9.7h and 0.9.8 before 0.9.8a, when using the SSL_OP_MSIE_SSLV2_RSA_PADDING option, disables a verification step that is required for preventing protocol version rollback attacks, which allows remote attackers to force a client and server to use a weaker protocol than needed via a man-in-the-middle attack.

CVE-2005-2969 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2007-2457
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF hitachi-hicommand-security-bypass(35287)
About Security Update 2005-009	web.archive.org text/html Inactive Link Not Archived	APPLE APPLE-SA-2005-11-29
	Patch Vendor Advisory www.openssl.org text/plain	CONFIRM www.openssl.org/news/secadv_20051011.txt

Juniper IVE OS Potential SSL 2.0 Rollback Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 18123
SecurityTracker.com Archives - OpenSSL SSL_OP_MSIE_SSLV2_RSA_PADDING Option May Let Remote Users Rollback the Protocol Version	securitytracker.com text/html	SECTRACK 1015032
Secunia - Advisories - Ubuntu update for openssl	web.archive.org text/html	SECUNIA 17189
Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities	web.archive.org text/html	SECUNIA 17813
Debian -- Security Information -- DSA-881-1 openssl096	www.debian.org Depreciated Link text/html	DEBIAN DSA-881
Support	www.redhat.com text/html	REDHAT RHSA-2005:762
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2036
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-3056
Secunia - Advisories - IBM HMC OpenSSL Vulnerabilities	web.archive.org text/html	SECUNIA 18165
IBM Director OpenSSL Potential SSL 2.0 Rollback Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 21827
Secunia - Advisories - Serv-U FTP Server Potential Denial of Service Vulnerability	web.archive.org text/html	SECUNIA 17409
Support	www.redhat.com text/html	REDHAT RHSA-2008:0629
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2005:061
Debian -- Security Information -- DSA-875-1 openssl094	www.debian.org Depreciated Link text/html	DEBIAN DSA-875
rPath update for openssl - Advisories - Secunia	web.archive.org text/html	SECUNIA 26893
Secunia - Advisories - Red Hat update for openssl	web.archive.org text/html	SECUNIA 17153
Multiple Vulnerabilities of Hitachi Web Server: Software Vulnerability Information: Software: Hitachi	www.hitachi-support.com text/html	CONFIRM www.hitachi-support.com/security_e/vuls_e/HS06-022_e/01-e.html
rhn.redhat.com | Red Hat Support	Vendor Advisory www.redhat.com text/html	REDHAT RHSA-2005:800
Webmail : Solution de messagerie	www.vupen.com	VUPEN ADV-2007-0343

professionnelle - OVHcloud- OVH	text/html	
No Description Provided	issues.rpath.com Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-1633
TSLSA-2005-0059 - multi	web.archive.org text/html Inactive Link Not Archived	TRUSTIX TSLSA-2005-0059
	ftp.software.ibm.com text/plain Inactive Link Not Archived	MISC ftp.software.ibm.com/pc/pccbbs/pc_servers/dir5.10.3_docs_relnote
Secunia - Advisories - SmoothWall Express Update for Multiple Packages	web.archive.org text/html	SECUNIA 19185
1. Overview:	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-031.htm
Secunia - Advisories - Mandriva update for openssl	web.archive.org text/html	SECUNIA 17178
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	SECUNIA 17335
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2710
Secunia - Advisories - Debian update for openssl	web.archive.org text/html	SECUNIA 17344
Secunia - Advisories - Slackware update for openssl	web.archive.org text/html	SECUNIA 17191
NetBSD Update Fixes Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 17389
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-3002
IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	HP SSRT071299
OpenSSL Insecure Protocol Negotiation Weakness	cve.report (archive) text/html	BID 15071
Secunia - Advisories - Cisco Products OpenSSL Potential SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 17888
Secunia - Advisories - Sun Solaris OpenSSL SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 17169
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2659
IBM notice: The page you requested cannot be displayed	www-1.ibm.com text/html Inactive Link Not Archived	MISC www-1.ibm.com/support/docview.wss?uid=isg1SSRVHMCHMC_C081516_754
404 Not Found	www.juniper.net text/plain Inactive Link Not Archived	MISC www.juniper.net/support/security/alerts/PSN-2005-12-025
Cisco - Networking, Cloud, and Cybersecurity Solutions	www.cisco.com text/html	CISCO 20051202 Cisco Security Notice: Response to OpenSSL Potential SSL 2.0 Rollback

Secunia - Advisories - Blue Coat Products OpenSSL SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 17432
Secunia - Advisories - Avaya Intuity Audix OpenSSL Potential SSL 2.0 Rollback	web.archive.org text/html	SECUNIA 18663
Hitachi JP1/HiCommand Series Two Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 25973
Secunia - Advisories - Fedora update for openssl/openssl096b/openssl097a	web.archive.org text/html	SECUNIA 17210
Secunia - Advisories - Trustix update for multiple packages	web.archive.org text/html	SECUNIA 17288
Astaro Security Linux ISAKMP and SSL 2.0 Rollback Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 17617
Secunia - Advisories - OpenSSL Potential SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 17151
ASA-2006-260 HP-UX OpenSSL Denial of Service (DoS), Increase Privilige (HPSBUX02174)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-260.htm
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2908
JP1/HiCommand Series Products OpenSSL Insecure Protocol Negotiation Weakness	cve.report (archive) text/html	BID 24799
HP-UX update for OpenSSL - Advisories - Secunia	web.archive.org text/html	SECUNIA 23280
Secunia - Advisories - SUSE update for openssl	web.archive.org text/html	SECUNIA 17259
Protocol-version Rollback Vulnerability in OpenSSL of JP1/HiCommand Series Products: Software Vulnerability Information: Software: Hitachi	www.hitachi-support.com text/html	CONFIRM www.hitachi-support.com/security_e/vuls_e/HS07-016_e/index-e.html
Secunia - Advisories - Gentoo update for openssl	web.archive.org text/html	SECUNIA 17180
Hitachi Web Server Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 23843
Avaya PDS HP-UX Secure Shell / OpenSSL Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 23340
#101974: OpenSSL (see openssl(5)) May Allow an Agent to Force a Rollback to a Cryptographically Weak Protocol Version	web.archive.org text/html Inactive Link Not Archived	SUNALERT 101974
Secunia - Advisories - HP Web-Enabled Management Software Potential SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 18045
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2007-0326

IT Resource Center - login / register	web.archive.org text/html Inactive Link Not Archived	HP HPSBUX02174
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11454
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community	web.archive.org text/html	SECUNIA 31492
Secunia - Advisories - Astaro WebAdmin SSL 2.0 Rollback Vulnerability	web.archive.org text/html	SECUNIA 17466
Secunia - Advisories - Astaro WebAdmin SSL 2.0 Rollback and PPTP Denial of Service	web.archive.org text/html	SECUNIA 17632
Secunia - Advisories - UnixWare update for openssl	web.archive.org text/html	SECUNIA 17589
Debian -- Security Information -- DSA-882-1 openssl095	www.debian.org Depreciated Link text/html	DEBIAN DSA-882
HP-UX update for Apache - Advisories - Secunia	web.archive.org text/html	SECUNIA 23915
RETIRED: Apple Mac OS X Security Update 2005-009 Multiple Vulnerabilities	cve.report (archive) text/html	BID 15647
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2005:179
Secunia - Advisories - FreeBSD update for openssl	web.archive.org text/html	SECUNIA 17146
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-3531

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All

Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7a:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7b:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7c:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7d:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7e:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7f:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7g:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7a:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7b:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7c:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7d:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7e:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7f:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.7g:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:*:*:

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report