



CVE-2006-3738

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2006-3738
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-28 18:07:00 UTC
Updated	2018-10-17 21:29:00 UTC
Description	Buffer overflow in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 before 0.9.7i, 0.9.8 before 0.9.8d, and earlier ve

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

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	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	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	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All

References

Reference

Repository / Oval Repository

Kolab Server Multiple Vulnerabilities - Advisories - Secunia

SnapGear Multiple Vulnerabilities - Advisories - Secunia

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia

HP System Management Homepage Apache and OpenSSL Vulnerabilities - Advisories - Secunia

FreeBSD update for openssl - Advisories - Secunia

Red Hat update for openssl - Advisories - Secunia

OpenSSL Multiple Vulnerabilities - Advisories - Secunia

The Slackware Linux Project: Slackware Security Advisories

Debian update for openssl096 - Advisories - Secunia

2006-0054

VMware ESX Server 2.5.3 Upgrade Patch 6 (for 2.5.3 Systems)

OpenSSL SSL_Get_Shared_Ciphers Buffer Overflow Vulnerability

SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia

Xerox ESS/ Network Controller OpenSSL Vulnerabilities - Advisories - Secunia

US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities

CVE-2006-0054: Multiple Vulnerabilities in OpenSSL

SUSE updates for openssl, openssl, and bind9 - Advisories - Secunia
SecurityTracker.com Archives - OpenSSL ASN.1 Bugs, SSL_get_shared_ciphers() Buffer Overflow, and SSLv2 Client Error Lets Remote Use
Support
Serv-U FTP Server OpenSSL Multiple Vulnerabilities - Advisories - Secunia
Webmail - OVH
VMware ESX Server 2.1.3 Upgrade Patch 4 (for 2.1.3 Systems)
SourceForge.net: SysAdmin Tools from ITeFlx: Files
rhn.redhat.com Red Hat Support
Oracle Products Multiple Vulnerabilities - Advisories - Secunia
Debian -- Security Information -- DSA-1185-2 openssl
Webmail - OVH
Download Patch ESX-9986131 for VMware ESX Server 3.0.1
VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia
NetBSD update for OpenSSL - Advisories - Secunia
Sun Grid Engine Multiple OpenSSL Vulnerabilities - Advisories - Secunia
Webmail - OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Serv-U Release Notes - Current
SUSE update for openssl - Advisories - Secunia
Security Announcement
Cisco - Networking, Cloud, and Cybersecurity Solutions
HP Tru64 UNIX Multiple SSL and BIND Vulnerabilities - Advisories - Secunia
SecurityFocus
APPLE-SA-2006-11-28 Security Update 2006-007
SecurityFocus
OpenBSD update for OpenSSL - Advisories - Secunia
Webmail - OVH
Oracle Critical Patch Update - January 2007
VMware ESX Server 2.5.4 Upgrade Patch 3 (for 2.5.4 Systems Only)
FreeBSD-SA-06:23
Mandriva update for openssl - Advisories - Secunia
#102668: Security Vulnerabilities In OpenSSL Affect Sun Grid Engine 5.3 and N1 Grid Engine 6.0
SecurityTracker.com Archives - Oracle Database and Other Products Have 52 Unspecified Vulnerabilities With Unspecified Impact
rPath update for openssl - Advisories - Secunia
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC
Repository / Oval Repository

IT Resource Center - login / register
Advisories - Mandriva Linux
20061001-01-P
HPSBMA02250 SSRT061275 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Execution of Arbitrary Code
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
[#RPL-613] openssl vulnerabilities including remote unauthorized access: CVE-2006-2937 CVE-2006-2940 CVE-2006-3738 CVE-2006-4343
usn/usn-353-1 - Ubuntu: Linux for human beings
www.openssl.org/news/secadv_20060928.txt
Security Announcement
US-CERT Vulnerability Note VU#547300
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Ubuntu update for openssl - Advisories - Secunia
Advisories - Mandriva Linux
IBM HMC OpenSSH / OpenSSL Vulnerabilities - Advisories - Secunia
Mandriva update for ntp - Advisories - Secunia
OpenPKG Corporation: Security: Security Advisories
Debian update for openssl - Advisories - Secunia
Cisco Security Response: Multiple Vulnerabilities in OpenSSL Library [Cisco GSS 4400 Series Global Site Selector Appliances] - Cisco Systems
OpenVPN 2.0.x Change Log
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Nortel Communication Server OpenSSL Vulnerability - Advisories - Secunia
Webmail - OVH
SecurityFocus
Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia
rPath update for openssl - Advisories - Secunia
ASA-2006-260 HP-UX OpenSSL Denial of Service (DoS), Increase Privilege (HPSBUX02174)
HP Insight Management Agents SSL Vulnerabilities - Advisories - Secunia
Nortel Products OpenSSL Vulnerability - Advisories - Secunia
Webmail - OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
29262
HP-UX update for OpenSSL - Advisories - Secunia
About the security content of Security Update 2006-007
Debian -- Security Information -- DSA-1195-1 openssl096

[Full-disclosure] [SECURITY] OpenSSL 0.9.8d and 0.9.7l released
cwRsync OpenSSL Vulnerabilities and OpenSSH Weakness - Advisories - Secunia
Avaya PDS HP-UX Secure Shell / OpenSSL Multiple Vulnerabilities - Advisories - Secunia
#102711: Security Vulnerabilities in OpenSSL May Lead to a Denial of Service (DoS) to Applications or Execution of Arbitrary Code With Elevat
Trustix updates for openssh and openssl - Advisories - Secunia
Gentoo update for openssl - Advisories - Secunia
Mandriva update for MySQL - Advisories - Secunia
OpenBSD 4.0 errata
www.xerox.com/downloads/usa/en/c/cert_ESSNetwork_XRX07001_v1.pdf
Sun Solaris OpenSSL Vulnerabilities - Advisories - Secunia
404 Not Found
Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities
Gentoo update for emul-linux-x86-baselibs - Advisories - Secunia
Gentoo Linux Documentation -- AMD64 x86 emulation base libraries: OpenSSL multiple vulnerabilities
IT Resource Center - login / register
Slackware update for openssl - Advisories - Secunia
SSRT071304
Advisories - Mandriva Linux
Download Patch ESX-3069097 for VMware ESX Server 3.0.1
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
201531
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community
Nortel: Technical Support
Gentoo Itsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
SecurityFocus
IBM X-Force Exchange
Oracle January 2007 Security Update Multiple Vulnerabilities
Webmail - OVH
FileZilla / FileZilla Server Multiple Vulnerabilities - Advisories - Secunia
HP-UX update for Apache - Advisories - Secunia
VMware ESX Server 2.0.2 Upgrade Patch 4 (for 2.0.2 Systems)
ASA-2006-220 (RHSA-2006-0695)
NetBSD-SA2008-007
Avaya Products OpenSSL Multiple Vulnerabilities - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

Legacy QID Mappings

[390284](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

© [CVE.report](#) 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.
CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).
CVE.report and Source URL Uptime Status [status.cve.report](#)