



CVE-2006-2940

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

Summary

CVE	CVE-2006-2940
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-28 18:07:00 UTC
Updated	2018-10-18 16:44:00 UTC
Description	OpenSSL 0.9.7 before 0.9.7i, 0.9.8 before 0.9.8d, and earlier versions allows attackers to cause a denial of service (CPU c

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All

Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	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
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All

Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	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

[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](#)

[VMware Workstation 6 Release Notes](#)

[OpenSSL Multiple Vulnerabilities - Advisories - Secunia](#)

[The Slackware Linux Project: Slackware Security Advisories](#)

[Solaris OpenSSL Denial of Service Vulnerabilities - Advisories - Secunia](#)

[Debian update for openssl096 - Advisories - Secunia](#)

[2006-0054](#)

[VMware ESX Server 2.5.3 Upgrade Patch 6 \(for 2.5.3 Systems\)](#)

[SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Xerox ESS/ Network Controller OpenSSL Vulnerabilities - Advisories - Secunia](#)

[US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities](#)

[VMware Player Release Notes](#)

[SUSE updates for 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](#)

[FreeBSD-SA-06:23.openssl](#)

[VMware ESX Server 2.1.3 Upgrade Patch 4 \(for 2.1.3 Systems\)](#)

[SourceForge.net: SysAdmin Tools from ITeFlx: Files](#)

rPath update for openssl - Advisories - Secunia
rhn.redhat.com Red Hat Support
Oracle Products Multiple Vulnerabilities - Advisories - Secunia
Debian -- Security Information -- DSA-1185-2 openssl
Webmail - OVH
VMSA-2008-0005.1 - VMware
OpenSSL Public Key Processing Denial of Service Vulnerability
Download Patch ESX-9986131 for VMware ESX Server 3.0.1
usn/usn-353-2 - Ubuntu: Linux for human beings
VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia
VMware Server Release Notes
NetBSD update for OpenSSL - Advisories - Secunia
Sun Grid Engine Multiple OpenSSL Vulnerabilities - Advisories - Secunia
Webmail - OVH
Webmail - OVH
[Security-announce] VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion re
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Serv-U Release Notes - Current
issues.rpath.com/browse/RPL-1633
SUSE update for openssl - Advisories - Secunia
Webmail - OVH
Webmail - OVH
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)
29261
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 50 Unspecified Vulnerabilities With Unspecified Impact

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
IT Resource Center - login / register
Advisories - Mandriva Linux
20061001-01-P
201534
HPSBMA02250 SSRT061275 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Execution of Arbitrary Code
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
www.arkoon.fr/upload/alertes/37AK-2006-06-FR-1.1_FAST360_OPENSSL_ASN1.pdf
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Ubuntu update for openssl - Advisories - Secunia
www.uniras.gov.uk/niscc/docs/re-20060928-00661.pdf
Advisories - Mandriva Linux
Repository / Oval Repository
IBM HMC OpenSSH / OpenSSL Vulnerabilities - Advisories - Secunia
support.attachmate.com/techdocs/2374.html
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
Webmail - OVH
www.arkoon.fr/upload/alertes/41AK-2006-08-FR-1.1_SSL360_OPENSSL_ASN1.pdf
VMware Workstation 5.5 Release Notes
Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia
'Internet Systems Consortium Security Advisory. [revised]' - MARC
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
Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
HP-UX update for OpenSSL - Advisories - Secunia
About the security content of Security Update 2006-007
VMware ACE Release Notes
Debian -- Security Information -- DSA-1195-1 openssl096
VMware Player Release Notes
[Full-disclosure] [SECURITY] OpenSSL 0.9.8d and 0.9.7i released
cWRsync OpenSSL Vulnerabilities and OpenSSH Weakness - Advisories - Secunia
Avaya PDS HP-UX Secure Shell / OpenSSL Multiple Vulnerabilities - Advisories - Secunia
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
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
IBM X-Force Exchange
#102747: Security Vulnerabilities in OpenSSL May Lead to a Denial of Service (DoS) to Applications
Slackware update for openssl - Advisories - Secunia
SSRT071304
SecurityFocus
Advisories - Mandriva Linux
Download Patch ESX-3069097 for VMware ESX Server 3.0.1
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
VMware Server 1.0.5 and Workstation 6.0.3 Multiple Vulnerabilities
200585
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community
SecurityFocus
BIND OpenSSL Vulnerabilities - Advisories - Secunia
Oracle January 2007 Security Update Multiple Vulnerabilities
FileZilla / FileZilla Server Multiple Vulnerabilities - Advisories - Secunia

HP-UX update for Apache - Advisories - Secunia

Reflection for Secure IT Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

VMware ESX Server 2.0.2 Upgrade Patch 4 (for 2.0.2 Systems)

ASA-2006-220 (RHSA-2006-0695)

NetBSD-SA2008-007

Webmail - OVH

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](#)