CVE-2007-5135

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2007-5135
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-27 20:17:00 UTC
Updated	2018-10-15 21:40:00 UTC
Description	Off-by-one error in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 up to 0.9.7l, and 0.9.8 up to 0.9.8f, might allow

Risk And Classification

Problem Types: CWE-189

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	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	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	0.9.7l	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	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	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	0.9.7l	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	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All

References

Reference
OpenBSD 4.0 errata
www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd
VUPEN Security - Offensive Cyber Security
VMware ESXi OpenSSL Vulnerabilities - Advisories - Secunia
Webmail | OVH- OVH
OpenBSD 4.2 errata
SecurityFocus
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com
USN-522-1: openssl vulnerabilities | Ubuntu security notices
OpenSSL Multiple Vulnerabilities - Advisories - Secunia
issues.rpath.com/browse/RPL-1769
rhn.redhat.com | Red Hat Support
SecurityFocus
www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd
OpenBSD 4.1 errata
VMSA-2008-0001.1 - VMware
VMware ESX Server Multiple Security Updates - Advisories - Secunia
SecurityFocus
[security-announce] SUSE Security Summary Report SUSE-SR:2008:005
Security Advisories | Mandriva Linux
rPath update for openssl - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo Bug 194039 - dev-libs/openssl < 0.9.8e-r3 SSL_get_shared_ciphers() Off-by-One buffer underflow (CVE-2007-5135)
NetBSD update for OpenSSL - Advisories - Secunia
SUSE Update for Multiple Packages - Advisories - Secunia
VMSA-2008-0013.3 - VMware
Webmail | OVH- OVH
Debian update for openssl - Advisories - Secunia
[Security-announce] VMSA-2008-0001 Moderate OpenPegasus PAM Authentication Buffer Overflow and updated service console packages
FreeBSD-SA-07:08
Mandriva update for openssl - Advisories - Secunia
ASA-2007-485 (RHSA-2007-0813)
Debian -- Security Information -- DSA-1379-1 openssl

IBM X-Force Exchange
#200858: Security Vulnerability in Solaris 10 OpenSSL SSL_get_shared_ciphers() Function
Webmail - OVH
APPLE-SA-2008-07-31 Security Update 2008-005
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.openssl.org/news/secadv_20071012.txt
Linux Terminal Server Project: Multiple vulnerabilities — Gentoo Linux Documentation
OpenSSL Off-by-one Overflow in SL_get_shared_ciphers() Lets Remote Users Execute Arbitrary Code - SecurityTracker
OpenBSD update for OpenSSL - Advisories - Secunia
SecurityReason - OpenSSL SSL_get_shared_ciphers() off-by-one buffer overflow
FreeBSD update for openssl - Advisories - Secunia
SecurityFocus
SecurityFocus
Repository / Oval Repository
OpenSSL SSL_Get_Shared_Ciphers Off-by-One Buffer Overflow Vulnerability
Security Announcement
SecurityFocus
Webmail - OVH
#103130: Security Vulnerability in Solaris 10 OpenSSL SSL_get_shared_ciphers() Function
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rPath update for openssl - Advisories - Secunia
Red Hat update for openssl - Advisories - Secunia
Webmail - OVH
Sun Solaris 10 OpenSSL "SSL_get_shared_ciphers()" Vulnerability - Advisories - Secunia
IBM HMC Multiple Vulnerabilities - Advisories - Secunia
VMware updates for OpenSSL, net-snmp, and perl - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Repository / Oval Repository
rhn.redhat.com | Red Hat Support
Avaya Products OpenSSL Vulnerabilities - Advisories - Secunia
SecurityFocus
Gentoo ltsp Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo update for openssl - Advisories - Secunia
Ubuntu update for openssl - Advisories - Secunia
Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities
Fedora update for openssl - Advisories - Secunia

wiki.rpath.com/wiki/Advisories:rPSA-2008-0241
HP-UX update for Apache - Advisories - Secunia
[SECURITY] Fedora Core 6 Update: openssl-0.9.8b-15.fc6
NetBSD-SA2008-007
Red Hat update for openssl - Advisories - Secunia
rhn.redhat.com | Red Hat Support
issues.rpath.com/browse/RPL-1770
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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