CVE-2006-4343

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2006-4343
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 21:36:00 UTC
Description	The get_server_hello function in the SSLv2 client code in OpenSSL 0.9.7 before 0.9.7l, 0.9.8 before 0.9.8d, and earlier vers

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	5.04	All	All	All
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	5.04	All	All	All
Operating System	Canonical	Ubuntu Linux	5.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	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	0.9.7	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
29263
US-CERT Vulnerability Note VU#386964
Ingate Firewall and SIParator 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
OpenSSL < 0.9.7l / 0.9.8d SSLv2 Client Crash Exploit

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

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

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 openssh, 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 ITeF!x: Files

IBM X-Force Exchange

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

Release notice for Ingate Firewall® 4.5.2 and Ingate SIParator® 4.5.2

Download Patch ESX-9986131 for VMware ESX Server 3.0.1

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

[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

SUSE update for openssl - Advisories - Secunia

Security Announcement
Cisco - Networking, Cloud, and Cybersecurity Solutions
SecurityFocus
APPLE-SA-2006-11-28 Security Update 2006-007
SecurityFocus
Repository / Oval Repository
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)
Webmail - OVH
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
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 Cod
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
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Ubuntu update for openssl - Advisories - Secunia
Advisories - Mandriva Linux
IBM HMC OpenSSH / OpenSSL Vulnerabilities - Advisories - Secunia
OpenSSL SSLv2 Null Pointer Dereference Client Denial of Service Vulnerability
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 Syste
OpenVPN 2.0.x Change Log

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Repository / Oval Repository

VMware Workstation 5.5 Release Notes

Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia

rPath update for openssl - Advisories - Secunia

ASA-2006-260 HP-UX OpenSSL Denial of Service (DoS), Increase Privilige (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 0.9.7l 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 Eleva

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

SecurityFocus

Advisories - Mandriva Linux

Download Patch ESX-3069097 for VMware ESX Server 3.0.1

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

201521

201531
VMware Server 1.0.5 and Workstation 6.0.3 Multiple Vulnerabilities
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community
SecurityFocus
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
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)