CVE-2006-4339

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2006-4339
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-05 17:04:00 UTC
Updated	2018-10-17 21:35:00 UTC
Description	OpenSSL before 0.9.7, 0.9.7 before 0.9.7k, and 0.9.8 before 0.9.8c, when using an RSA key with exponent 3, removes PK(

Risk And Classification

Problem Types: CWE-310

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	0.9.7a	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	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	All	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	0.9.7a	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	0.9.8	All	All	All

Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All

References

Reference
Slackware update for bind - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
ASA-2006-188
Sybase Unwired Accelerator RSA Signature Forgery - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
#200474: Security Vulnerability With RSA Signature Affects the Sun Secure Global Desktop Software
#201390: Security Vulnerability With RSA Signature Affects Solaris Applications Utilizing the libike Library
Sun Java System Multiple Products RSA Signature Forgery - Advisories - Secunia
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia
HP System Management Homepage Apache and OpenSSL Vulnerabilities - Advisories - Secunia
[#RPL-616] openssl key forgery vulnerabilities for some RSA keys (CVE-2006-4339) - rPath JIRA
VMware Workstation 6 Release Notes
usn/usn-339-1 - Ubuntu: Linux for human beings
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
#102686: Security Vulnerability in RSA Signature Verification Affects Java 2 Platform, Standard Edition
Novell International Cryptographic Infrastructure Two Vulnerabilities - Advisories - Secunia
support.attachmate.com/techdocs/2127.html
VMware ESX Server 2.5.3 Upgrade Patch 6 (for 2.5.3 Systems)
Ubuntu update for openssl - Advisories - Secunia
Security Announcement
Security Announcement
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
#201247: Security Vulnerability With RSA Signatures Affects OpenSSL Shipped With Solaris
Sybase Afaria RSA Signature Forgery - Advisories - Secunia
US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities
VMware Player Release Notes
Reflection Products RSA Signature Forgery Vulnerability - Advisories - Secunia
SecureCRT / SecureFX OpenSSL RSA Signature Forgery - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Security Announcement

1000148

Gentoo Linux Documentation -- OpenSSL, AMD64 x86 emulation base libraries: RSA signature forgery

HP-UX update for Bind - Advisories - Secunia

Support

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

HP-UX update for firefox - Advisories - Secunia

Red Hat update for java-1.4.2-ibm - Advisories - Secunia

OpenVPN Multiple Vulnerabilities - Advisories - Secunia

Serv-U FTP Server OpenSSL Multiple Vulnerabilities - Advisories - Secunia

VMware ESX Server 2.1.3 Upgrade Patch 4 (for 2.1.3 Systems)

The Slackware Linux Project: Slackware Security Advisories

rhn.redhat.com | Red Hat Support

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

rPath update for openssl - Advisories - Secunia

Oracle Products Multiple Vulnerabilities - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

VMSA-2008-0005.1 - VMware

Download Patch ESX-9986131 for VMware ESX Server 3.0.1

VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia

VMware Server Release Notes

OpenSSL RSA Signature Forgery Vulnerability - Advisories - Secunia

Red Hat update for openssl - Advisories - Secunia

Gentoo update for openssl - Advisories - Secunia

Sun Solaris WAN Boot RSA Signature Forgery Vulnerability - Advisories - Secunia

Security Advisory SA60799 - Gentoo openoffice Multiple Vulnerabilties - Secunia

[Security-announce] VMSA-2008-0005 Updated VMware Workstation, VMware Player, VMware Server, VMware ACE, and VMware Fusion re

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Serv-U Release Notes - Current

issues.rpath.com/browse/RPL-1633

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Debian update for openssl096 - Advisories - Secunia

SecurityTracker.com Archives - OpenSSL RSA Signatures Can Be Forged

Cisco - Networking, Cloud, and Cybersecurity Solutions

Cisco - Networking, Cloud, and Cybersecurity Solutions

HP Tru64 UNIX Multiple SSL and BIND Vulnerabilities - Advisories - Secunia

Gentoo Linux Documentation -- Mozilla Network Security Service (NSS): RSA signature forgery

APPLE-SA-2006-11-28 Security Update 2006-007

OpenOffice.org 3 Multiple Vulnerabilities - Advisories - Community

JVN#51615542: Adobe Reader fails to properly handle signatures

Oracle Critical Patch Update - January 2007

VMware ESX Server 2.5.4 Upgrade Patch 3 (for 2.5.4 Systems Only)

Bleichenbacher's RSA signature forgery based on implementation error

Repository / Oval Repository

SecurityTracker.com Archives - Oracle Database and Other Products Have 52 Unspecified Vulnerabilities With Unspecified Impact

OpenSSL PKCS Padding RSA Signature Forgery Vulnerability

Support

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC

Sun JES / Solaris OpenSSL RSA Signature Forgery - Advisories - Secunia

OpenOffice.org 2 Multiple Vulnerabilities - Advisories - Community

CVE-2006-4339

Mandriva update for openssl - Advisories - Secunia

IT Resource Center - login / register

Gentoo update for opera - Advisories - Secunia

APPLE-SA-2007-12-14 Java Release 6 for Mac OS X 10.4

Advisories - Mandriva Linux

Debian update for openssl - Advisories - Secunia

201534

HPSBMA02250 SSRT061275 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Execution of Arbitrary Cod

SSRT061273

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

secure-support.novell.com/KanisaPlatform/Publishing/41/3143224_f.SAL_Public.html

SUSE update for openssl/mozilla-nss - Advisories - Secunia

IBM X-Force Exchange

Webmail - OVH

Advisories - Mandriva Linux

FreeBSD update for openssl - Advisories - Secunia

IBM - Subscription service - Bulletin

Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

FreeBSD-SA-06:19

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Oracle Open Office Multiple Vulnerabilities - Advisories - Community

Advisories - Mandriva Linux

JVNDB-2012-000079

US-CERT Vulnerability Note VU#845620

Mandriva update for ntp - Advisories - Secunia

Slackware update for openssl - Advisories - Secunia

WebLogic SSL may verify RSA Signatures incorrectly if the RSA key exponent is 3

Cisco Security Response: Multiple Vulnerabilities in OpenSSL Library [Cisco GSS 4400 Series Global Site Selector Appliances] - Cisco Syste

OpenVPN 2.0.x Change Log

#200708: A Security Vulnerability in RSA Signature Verification Affects Sun Java System Application Server, Proxy Server and Web Server

Sybase PowerBuilder RSA Signature Forgery - Advisories - Secunia

Gentoo update for nss - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Opera SSL RSA Signature Forgery Vulnerability - Advisories - Secunia

OpenPKG Corporation: Security: Security Advisories

Gentoo Linux Documentation -- OpenOffice, LibreOffice: Multiple vulnerabilities

SecurityFocus

Webmail - OVH

Sybase Enterprise Portal RSA Signature Forgery - Advisories - Secunia

Preliminary advisory on security vulnerability in RSA signature verification impacting several Sybase products - Sybase Inc

VMware Workstation 5.5 Release Notes

Gentoo Linux Documentation -- Opera: RSA signature forgery

Blue Coat Support - Security Advisories

SUSE Update for Multiple Packages - Advisories - Secunia

Cisco Products OpenSSL Vulnerabilities - Advisories - Secunia

Support

'Internet Systems Consortium Security Advisory. [revised]' - MARC

200708

HP Insight Management Agents SSL Vulnerabilities - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Sybase mFolio RSA Signature Forgery - Advisories - Secunia

20060901-01-P

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SUSE update for opera - Advisories - Secunia

Debian -- Security Information -- DSA-1173-1 openssl

About the security content of Security Update 2006-007

Advisories - Mandriva Linux

OpenVPN OpenSSL RSA Signature Forgery - Advisories - Secunia

VMware ACE Release Notes

Juniper Secure Access / Unified Access Control RSA Signature Forgery - Advisories - Secunia

Mozilla Firefox Multiple Vulnerabilities - Advisories - Secunia

Blue Coat Products RSA Signature Vulnerability - Advisories - Secunia

VMware Player Release Notes

OpenBSD update for OpenSSL - Advisories - Secunia

Opera Software - Knowledge Base

OpenBSD 4.0 errata

www.openssl.org/news/secadv_20060905.txt

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Sybase Mach Desktop RSA Signature Forgery - Advisories - Secunia

#102759: Security Vulnerability With RSA Signatures Affects Solaris WAN Boot

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Mandriva update for MySQL - Advisories - Secunia

201247

Avaya Products OpenSSL Vulnerability - Advisories - Secunia

BEA Products Multiple Vulnerabilities - Advisories - Secunia

#200610: Security Vulnerability Issue of Forged RSA Signatures for Java Enterprise System and Solaris

Ingate Firewall and SIParator OpenSSL Vulnerability - Advisories - Secunia

OpenPKG Corporation: Security: Security Advisories

Mandriva update for bind - Advisories - Secunia

#102648: Security Vulnerability in RSA Signature Verification Impacting Multiple SUN Products

Security Announcement

Reflection Security Updates for US-CERT Vulnerability #845620: RSA Public Exponent 3 - Tech Note 2137

Sun Secure Global Desktop Software RSA Signature Forgery Vulnerability - Advisories - Secunia

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

IBM HMC Apache2 / OpenSSL Vulnerabilities - Advisories - Secunia

SSRT071304

SSRT071304
SecurityFocus
Mac OS X Java Multiple Vulnerabilities - Advisories - Secunia
Download Patch ESX-3069097 for VMware ESX Server 3.0.1
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Matasano Chargen » Many RSA Signatures May Be Forgeable In OpenSSL and Elsewhere
VMware Server 1.0.5 and Workstation 6.0.3 Multiple Vulnerabilities
Red Hat Network Satellite Server Update for Solaris Client - Advisories - Community
Debian -- Security Information -- DSA-1174-1 openssl096
SecurityFocus
BIND OpenSSL Vulnerabilities - Advisories - Secunia
Oracle January 2007 Security Update Multiple Vulnerabilities
IT Resource Center - login / register
HP-UX update for Apache - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Sybase RFID Enterprise RSA Signature Forgery - Advisories - Secunia
VMware ESX Server 2.0.2 Upgrade Patch 4 (for 2.0.2 Systems)
Sun Solaris RSA Signature Forgery Vulnerability - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories
About the security content of Java Release 6 for Mac OS X 10.4
support.attachmate.com/techdocs/2128.html
www.arkoon.fr/upload/alertes/40AK-2006-04-FR-1.1_SSL360_OPENSSL_RSA.pdf
Support
Webmail - OVH
28549
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rPath update for openssl - Advisories - Secunia
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	Vulnerable. This issue affects OpenSSL and OpenSSL compatibility packages in Red Hat Enterp

Legacy QID Mappings

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

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