



CVE-2010-3864

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

Summary

CVE	CVE-2010-3864
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-17 16:00:00 UTC
Updated	2023-02-13 04:27:00 UTC
Description	Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and intern...

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	0.9.8g	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All

Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All

References

Reference

Security Advisory SA57353 - IBM Storage System DS8870 OpenSSL Multiple Vulnerabilities - Secunia

APPLE-SA-2011-06-23-1 Mac OS X v10.6.8 and Security Update 2011-004

IBM Security Bulletin: Storage HMC OpenSSL upgrade to address cryptographic vulnerabilities. - United States

HPSBMA02658

HP Insight Control for Linux Multiple Vulnerabilities - Secunia.com

[syslog-ng-announce] syslog-ng Premium Edition 3.2.1a has been released

Debian update for openssl - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Red Hat Customer Portal

access.redhat.com | CVE-2010-3864

Debian -- Security Information -- DSA-2125-1 openssl

SecurityFocus

VMware ESX Server / ESXi OpenSSL Vulnerabilities - Secunia.com

Slackware update for openssl - Secunia.com

VMSA-2011-0003

rhn.redhat.com | Red Hat Support

[SECURITY] Fedora 12 Update: openssl-1.0.0b-1.fc12

FreeBSD-SA-10:10

OpenSSL TLS Server Extension Parsing Race Condition Vulnerability - Advisories - Community

About the security content of Mac OS X v10.6.8 and Security Update 2011-004 - Apple Support

[SECURITY] Fedora 13 Update: openssl-1.0.0b-1.fc13

Adobe - Security Bulletins: APSB11-11 - Security update available for Adobe Flash Media Server

404 Not Found

'[security bulletin] HPSBUX02638 SSRT100339 rev.1 - HP-UX Running OpenSSL, Remote Execution of Arbitr' - MARC

Bug 649304 – CVE-2010-3864 OpenSSL TLS extension parsing race condition

Security Tracker.com Archives - OpenSSL Buffer Overflow in TLS Server Extension Parsing May Let Remote Users Execute Arbitrary Code

Ubuntu update for openssl - Advisories - Community

Security Alerts - Secunia

openssl.org/news/secadv_20101116.txt

SUSE Update for Multiple Packages - Secunia.com

The Slackware Linux Project: Slackware Security Advisories

'[security bulletin] HPSBGN02740 SSRT100741 rev.1 - HP Operations Manager, Operations Agent, Performa' - MARC

[SECURITY] Fedora 14 Update: openssl-1.0.0b-1.fc14

[syslog-ng-announce] syslog-ng Premium Edition 3.0.6a has been released

FreeBSD update for openssl - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:022

'[security bulletin] HPSBOV02670 SSRT100475 rev.1 - HP OpenVMS running SSL, Remote Denial of Service' - MARC

Vulnerability Note VU#737740 - Fiery Network Controllers for Xerox DocuColor 242/252/260 Printer/Copier use a vulnerable version of OpenSSL

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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)

© [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](#)