



CVE-2009-1379

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2009-1379
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-19 19:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allow

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

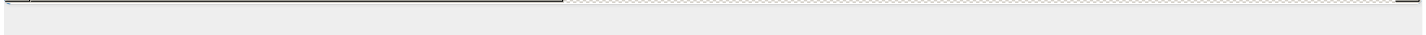
Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All

References

Reference

- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- kb.bluecoat.com/index
- Bug 501572 – CVE-2009-1379 OpenSSL: DTLS pointer use-after-free flaw (DoS)
- HPSBMA02492 SSRT100079 rev.1 - HP System Management Homepage (SMH) for Linux and Windows, Remote Cross Site Scripting (XSS)
- VooDoo cIRClE security advisory 20091012-01
- Ubuntu update for openssl - Secunia.com
- About Secunia Research | Flexera
- oss-security - Re: Two OpenSSL DTLS remote DoS
- Fedora update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com
- Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
- IBM X-Force Exchange
- Repository / Oval Repository

Red Hat Customer Portal
About Secunia Research Flexera
Page not found - SourceForge.net
Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities
CVE-2009-1379
Slackware update for openssl - Advisories - Community
SUSE Update for Multiple Packages - Advisories - Community
NetBSD update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com
NetBSD-SA2009-009
SecurityTracker.com Archives - OpenSSL DTLS Processing Bugs Let Users Deny Service
access.redhat.com CVE-2009-1379
VMware vMA Update for Multiple Packages - Advisories - Community
VooDoo cIRcLe OpenSSL DTLS Denial of Service Vulnerabilities - Secunia.com
The Slackware Linux Project: Slackware Security Advisories
#1923: dtls1_retrieve_buffered_fragment: Read from freed data structure
Support
[Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates
USN-792-1: OpenSSL vulnerabilities Ubuntu
OpenSSL 'dtls1_retrieve_buffered_fragment()' DTLS Packet Denial of Service Vulnerability
VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community
Repository / Oval Repository
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:011
Secunia Advisories - Vulnerability Information - Secunia.com
CVE Program record
NVD vulnerability detail



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-02	Tomas Hoger	This issue did not affect versions of openssl as shipped in Red Hat Enterprise Linux 3 and 4. T



Legacy QID Mappings

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

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](#)