



# CVE-2009-1377

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

## Summary

<b>CVE</b>	CVE-2009-1377
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-05-19 19:30:00 UTC
<b>Updated</b>	2022-02-02 15:07:00 UTC
<b>Description</b>	The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to ca

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	-	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta4	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta5	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	beta6	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8c-1	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8g-9	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8j	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-1	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-2	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-3	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-4	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-5	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-6	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-7	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-8	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8c-9	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-1	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-2	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-3	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-4	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-5	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-6	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-7	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-8	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8d-9	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8e-1	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8e-2	All	All	All





Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8g-7	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8g-8	All	All	All
Application	<a href="#">Openssl Project</a>	<a href="#">Openssl</a>	0.9.8g-9	All	All	All

## References

### Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[kb.bluecoat.com/index](http://kb.bluecoat.com/index)

Support / Security / Advisories // MDVSA-2009:120 | Mandriva

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

#1930: [PATCH] DTLS record buffer limitation bug

Repository / Oval Repository

About Secunia Research | Flexera

Fedora update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

oss-security - Two OpenSSL DTLS remote DoS

OpenSSL DTLS Denial of Service Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

About Secunia Research | Flexera

Page not found - SourceForge.net

Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities

OpenSSL DTLS Packets Multiple Denial of Service Vulnerabilities

CVE-2009-1377

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

'[openssl.org #1930] [PATCH] DTLS record buffer limitation bug' - MARC

SecurityTracker.com Archives - OpenSSL DTLS Processing Bugs Let Users Deny Service

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

[cvs.openssl.org/chngview](http://cvs.openssl.org/chngview)

Support

Security announced VMware 2010-0004 ESX Service Console and vMA third party updates

[security-announce] VMMSA-2010-0004 ESX Service Console and vMA third party updates

USN-792-1: OpenSSL vulnerabilities | Ubuntu

Repository / Oval Repository

VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community

[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)

© [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](#)