



# CVE-2011-4108

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

## Summary

<b>CVE</b>	CVE-2011-4108
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-01-06 01:55:00 UTC
<b>Updated</b>	2016-08-23 02:04:00 UTC
<b>Description</b>	The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is

## 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	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	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	0.9.6h	bogus	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.6m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7b	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.7m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8	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</a>	<a href="#">Openssl</a>	0.9.8k	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8l	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8m	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8n	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8o	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8p	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	0.9.8q	All	All	All

Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All
Application	Openssl	Openssl	1.0.0d	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	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6a	All	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	0.9.6h	bogus	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	0.9.7	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	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	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	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	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	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0c	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0d	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	All	All	All	All

## References

### Reference

HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Ur

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

[security-announce] SUSE-SU-2012:0084-1: important: Security update for

Red Hat Customer Portal

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

Red Hat Customer Portal

[security-announce] SUSE-SU-2014:0320-1: critical: Security update for g

CVE-2011-4108 OpenSSL Plain Text Recovery Attack Vulnerability

'[security bulletin] HPSBUX02734 SSRT100729 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

[SECURITY] Fedora 18 Update: mingw-openssl-1.0.1c-1.fc18

[aix.software.ibm.com/aix/efixes/security/openssl\\_advisory3.asc](http://aix.software.ibm.com/aix/efixes/security/openssl_advisory3.asc)

[security-announce] openSUSE-SU-2012:0083-1: important: openssl: fixing

Security Alerts - Secunia

[www.isg.rhul.ac.uk/~kp/dtls.pdf](http://www.isg.rhul.ac.uk/~kp/dtls.pdf)

Debian -- Security Information -- DSA-2390-1 openssl

APPLE-SA-2013-06-04-1 OS X Mountain Lion v10.8.4 and Security Update 2013-002

Red Hat Customer Portal

'[security bulletin] HPSBMU02776 SSRT100852 rev.1 - HP Onboard Administrator (OA), Remote Unauthorize' - MARC

Support / Security / Advisories // MDVSA-2012:006 | Mandriva

Security Advisory SA57260 - SUSE update for gnutls - Secunia

Support / Security / Advisories // MDVSA-2012:007 | Mandriva

About the security content of OS X Mountain Lion v10.8.4 and Security Update 2013-002

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

[www.openssl.org/news/secadv\\_20120104.txt](http://www.openssl.org/news/secadv_20120104.txt)

'[security bulletin] HPSBOV02793 SSRT100891 rev.1 - HP OpenVMS running SSL, Remote Denial of Service' - MARC

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[390226](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

[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](#)