



# CVE-2015-1788

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

## Summary

<b>CVE</b>	CVE-2015-1788
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-06-12 19:59:00 UTC
<b>Updated</b>	2022-12-13 12:15:00 UTC
<b>Description</b>	The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1

## Risk And Classification

### Problem Types: CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta2	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta3	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta4	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0	beta5	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0a	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	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>	1.0.0e	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0f	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0g	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0h	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0i	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0j	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.0k	All	All	All

Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All
Application	Openssl	Openssl	1.0.0q	All	All	All
Application	Openssl	Openssl	1.0.0r	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	All	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	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All
Application	Openssl	Openssl	1.0.0q	All	All	All
Application	Openssl	Openssl	1.0.0r	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1	beta1	All	All
Application	Openssl	Openssl	1.0.1	beta2	All	All
Application	Openssl	Openssl	1.0.1	beta3	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.1m	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All

Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2	beta1	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.2a	All	All	All

## References

### Reference

FortiGuard

NetBSD-SA2015-008

Oracle Critical Patch Update - July 2016

OpenSSL Bugs Let Remote Users Deny Service and Potentially Execute Arbitrary Code - SecurityTracker

IBM Security Bulletin: Vulnerabilities in OpenSSL including Logjam affect IBM Tivoli Netcool System Service Monitors/Application Service Monitors

Oracle July 2016 Critical Patch Update Multiple Vulnerabilities

USN-2639-1: OpenSSL vulnerabilities | Ubuntu

Oracle Critical Patch Update - October 2015

bn/bn\_gf2m.c: avoid infinite loop with malformed ECPParameters. · openssl/openssl@4924b37 · GitHub

Document Display | HPE Support Center

FortiGuard

OpenSSL: Multiple vulnerabilities (GLSA 201506-02) — Gentoo security

Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware

75158

About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support

openssl.org/news/secadv/20150611.txt

Document Display | HPE Support Center

'[security bulletin] HPSB MU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC

[security-announce] SUSE-SU-2015:1185-1: important: Security update for

Oracle Critical Patch Update - October 2016

Document Display | HPE Support Center

Broadcom Support Portal

Multiple Vulnerabilities in OpenSSL (June 2015) Affecting Cisco Products

[security-announce] SUSE-SU-2015:1143-1: important: Security update for

'[security bulletin] HPSB MU03388 SSRT102180 rev.1 - HP-UX running OpenSSL, Remote Disclosure of Information' - MARC

FortiGuard

Oracle Solaris Third Party Bulletin - July 2015

www.openssl.org/news/secadv\_20150611.txt

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

[security-announce] SUSE-SU-2015:1182-1: important: Security update for

[security-announce] SUSE-SU-2015:1184-1: important: Security update for

APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006

[security-announce] openSUSE-SU-2015:1277-1: important: Security update

FortiGuard

[security-announce] openSUSE-SU-2016:0640-1: important: Security update

[security-announce] SUSE-SU-2015:1150-1: important: Security update for

Debian -- Security Information -- DSA-3287-1 openssl

Document Display | HPE Support Center

McAfee KnowledgeBase - Intel Security - Security Bulletin: Seven OpenSSL CVEs Announced on June 11, 2015

Document Display | HPE Support Center

[security-announce] SUSE-SU-2015:1181-1: important: Security update for

Oracle Critical Patch Update - July 2017

Juniper Networks - 2015-10 Security Bulletin: Junos: OpenSSL June-July 2015 advisories - Knowledge Base

Oracle Critical Patch Update - October 2017

[security-announce] openSUSE-SU-2015:1139-1: important: Security update

Oracle Critical Patch Update - January 2016

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[591280](#) Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)

[591311](#) Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)

© [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](#)**