CVE-2014-0195

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-0195
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-05 21:55:00 UTC
Updated	2023-11-07 02:18:00 UTC
Description	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	All	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	All	All	All	All
Application	Mariadb	Mariadb	All	All	All	All
Application	Openssl	Openssl	All	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	0.9.8m	beta1	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	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	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	1.0.1	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	All	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	0.9.8m	beta1	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	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All

Application	Openssl	Openssl	0.9.8x	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	1.0.1	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
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Application	Redhat	Storage	2.1	All	All	All
Application	Redhat	Storage	2.1	All	All	All

References

Reference
Security Advisory SA59530 - BlackBerry Link OpenSSL Two Vulnerabilities - Secunia
kb.bluecoat.com/index
Security Advisory SA59040 - Cisco AnyConnect VPN Client OpenSSL Multiple Vulnerabilities - Secunia
'[security bulletin] HPSBHF03293 rev.1 - HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and' - MARC
'[security bulletin] HPSBGN03050 rev.1 - HP IceWall SSO Dfw and HP IceWall MCRP running OpenSSL, Remo' - MARC
Security Advisory SA59223 - F-Secure E-mail and Server Security / Server Security OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA59301 - HP Version Control Repository Manager (VCRM) OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA58977 - IBM BladeCenter Advanced Management Module Firmware OpenSSL Multiple Vulnerabilities - Secunia
ZDI-14-173/CVE-2014-0195 - OpenSSL DTLS Fragment O... - HP Enterprise Business Community
Security Advisory SA59162 - McAfee Multiple Products OpenSSL Multiple Vulnerabilities - Secunia
IBM Security Bulletin: IBM Tivoli Netcool System Service Monitors/Application Service Monitors is affected by the following OpenSSL vulnerab
Security Advisory SA58945 - IBM FastSetup OpenSSL Multiple Vulnerabilities - Secunia
IBM Se curity Bulletin: Tivoli Workload Scheduler is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE
OpenSSL DTLS Processing Bugs Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker
IBM notice: The page you requested cannot be displayed
About Secunia Research | Flexera
aix.software.ibm.com/aix/efixes/security/openssl_advisory9.asc
Security Advisory SA59342 - HP Smart Update Manager (HP SUM) OpenSSL Multiple Vulnerabilities - Secunia
About the security content of OS X Mavericks v10.9.5 and Security Update 2014-004 - Apple Support
Security Advisory SA59451 - IBM Tivoli Composite Application Manager for Transactions OpenSSL Security Issue and Vulnerabilities - Secun
Security Advisory SA59514 - HP System Management Homepage OpenSSL Multiple Vulnerabilities - Secunia
FortiGuard.com | Multiple Vulnerabilities in OpenSSL
Security Advisory SA59192 - Cisco TelePresence Server OpenSSL Multiple Vulnerabilities - Secunia
IBM Security Bulletin: IBM Initiate Master Data Service, IBM InfoSphere Master Data Management are affected by the following OpenSSL vulr
Security Advisory SA59454 - Cisco Unity Connection OpenSSL Multiple Vulnerabilities - Secunia
Citrix Security Advisory for OpenSSL Vulnerabilities (June 2014)
Security Advisory SA59655 - IBM SmartCloud Provisioning for IBM Provided Software Virtual Appliance OpenSSL Multiple Vulnerabilities - Se
Security Advisory SA58660 - Cisco Multiple Products OpenSSL SSL/TLS Handshake and Buffer Overflow Vulnerabilities - Secunia
[SECURITY] Fedora 19 Update: openssl-1.0.1e-39.fc19
Security Advisory SA58743 - Fortinet FortiOS (FortiGate) OpenSSL Two Vulnerabilities - Secunia
Security Advisory SA59287 - IBM Proventia Network Enterprise Scanner OpenSSL Multiple Vulnerabilities - Secunia
IBM Security Bulletin: IBM InfoSphere Guardium Database Activity Monitor is affected by CVE-2014-0221, CVE-2014-0224, CVE-2014-0195,
VMSA-2014-0012 | United States

VMSA-2014-0012 | United States

Security Advisory SA59437 - IBM Rational Application Developer for WebSphere Software OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: Vulnerabilities in OpenSSL affect IBM SmartCloud Provisioning. - United States

Security Advisory SA59666 - IBM SDK for Node.js OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA59175 - HP OpenVMS update for SSL - Secunia

Security Advisory SA58713 - IBM Multiple Products OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM Security Proventia Network Enterprise Scanner is affected by the following OpenSSL vulnerabilities: CVE-2014-022

Security Advisory SA59450 - IBM API Management OpenSSL Multiple Vulnerabilities - Secunia

IBM notice: The page you requested cannot be displayed

IBM Security Bulletin: IBM i is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-201

www.mandriva.com

Security Bulletin: Rational Application Developer is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-

IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.3.0.1 Interim Fix 29 README Tivoli Composite Appl

Security Advisory SA59449 - IBM Security Network Intrusion Prevention System OpenSSL Multiple Vulnerabilities - Secunia

McAfee KnowledgeBase - McAfee Security Bulletin – Seven OpenSSL vulnerabilities patched in McAfee products

git.openssl.org Git - openssl.git/commit

Security Advisory SA59305 - IBM MessageSight Server OpenSSL SSL/TLS Handshake and Buffer Overflow Vulnerabilities - Secunia

Security Advisory SA58615 - IBM Tivoli Netcool System Service Monitors Multiple Security Issues and Multiple Vulnerabilities - Secunia

'[security bulletin] HPSBMU03057 rev.1 - HP Version Control Agent (HP VCA) running OpenSSL on Linux a' - MARC

'[security bulletin] HPSBMU03056 rev.1 - HP Version Control Repository Manager (HP VCRM) running Open' - MARC

'[security bulletin] HPSBMU03062 rev.1 - HP Insight Control server deployment on Linux and Windows ru' - MARC

Security Advisory SA59528 - BlackBerry Enterprise Service Universal Device Service Component OpenSSL Multiple Vulnerabilities - Secunia

git.openssl.org Git - openssl.git/commit

Oracle Critical Patch Update - January 2015

IBM Security Bulletin: IBM Security Network Intrusion Prevention System is affected by the following OpenSSL vulnerabilities: CVE-2014-0224

Security Advisory SA59587 - F5 Multiple Products OpenSSL "dtls1_reassemble_fragment()" Buffer Overflow Vulnerability - Secuni

Security Advisory SA60571 - EMC Documentum Content Server Multiple Vulnerabilities - Secunia

Security Advisory SA59669 - IBM InfoSphere Guardium OpenSSL Security Issue and Multiple Vulnerabilities - Secunia

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

Security Advisory SA59413 - IBM Initiate Master Data Service / IBM InfoSphere Master Data Management OpenSSL Vulnerabilities - Secunia

'[security bulletin] HPSBMU03074 rev.1 - HP Insight Control server migration on Linux and Windows run' - MARC

Security Advisory SA59300 - IBM Tivoli Management Framework OpenSSL Multiple Vulnerabilities - Secunia

[security-announce] SUSE-SU-2015:0743-1: important: Security update for

Security Advisory SA59365 - Cisco MDS 9000 / Nexus 7000 OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA59441 - IBM Tivoli Network Manager IP Edition OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA59518 - IBM Tivoli Workload Scheduler for Applications OpenSSL Multiple Vulnerabilities - Secunia

Document Display | HPE Support Center

'[security bulletin] HPSBMU03055 rev.1 - HP Smart Update Manager (HP SUM) running OpenSSL, Remote Den' - MARC

SOL15356 - OpenSSL vulnerability CVE-2014-0195

IBM Support

Security Advisory SA59990 - Cisco Quantum Policy Suite OpenSSL Multiple Vulnerabilities - Secunia

'[security bulletin] HPSBMU03069 rev.1 - HP Software Operation Orchestration, OpenSSL Vulnerability, ' - MARC

Security Advisory SA59659 - IBM Tivoli Workload Scheduler Distributed OpenSSL Multiple Vulnerabilities - Secunia

www.novell.com/support/kb/doc.php

Security Advisory SA59490 - HP Version Control Agent OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA58337 - IBM Upward Integration Modules (UIM) OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM® SDK for Node.js™ is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, CVE-2

Support / Security / Advisories / / MDVSA-2015:062 | Mandriva

'[security bulletin] HPSBMU03065 rev.1 - HP Operations Analytics, OpenSSL Vulnerability, SSL/TLS, Rem' - MARC

Security Advisory SA59784 - Novell File Reporter Multiple OpenSSL Vulnerabilities - Secunia

Security Advisory SA59721 - IBM SmartCloud Provisioning OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory-Multiple OpenSSL vulnerabilities on Huawei products - Huawei PSIRT

IBM Tivoli Composite Application Manager for Transactions Internet Service Monitoring 7.4 Interim Fix 13 README Tivoli Composite Applicati

About Secunia Research | Flexera

'[security bulletin] HPSBOV03047 rev.1 - HP OpenVMS running OpenSSL, Remote Denial of Service (DoS), ' - MARC

IBM Support

Security Advisory SA59188 - Blue Coat Multiple Products OpenSSL Two Vulnerabilities - Secunia

Multiple Vulnerabilities in OpenSSL Affecting Cisco Products

Security Advisory SA59429 - Cisco IOS OpenSSL Multiple Vulnerabilities - Secunia

'[security bulletin] HPSBUX03046 SSRT101590 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC

IBM notice: The page you requested cannot be displayed

www.openssl.org/news/secadv_20140605.txt

Gentoo Linux Documentation -- OpenSSL: Multiple vulnerabilities

OpenSSL CVE-2014-0195 Memory Corruption Vulnerability

Oracle Critical Patch Update - October 2014

Oracle Critical Patch Update - July 2014

IBM Security Bulletin: IBM MessageSight is affected by the following OpenSSL vulnerabilities: (CVE-2014-0224, and CVE-2014-0195) - Unitec

Juniper Networks - 2014-06 Out of Cycle Security Bulletin: Vulnerabilities in OpenSSL related to ChangeCipherSpec, DTLS, SSL_MODE_REI

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

'[security bulletin] HPSBMU03076 rev.2 - HP Systems Insight Manager (SIM) on Linux and Windows runnin' - MARC

'[security bulletin] HPSBMU03051 rev.2 - HP System Management Homepage running OpenSSL on Linux and W' - MARC

Security Advisory SA59310 - Novell Messenger OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: SmartCloud Orchestrator is affected by the following OpenSSL vulnerabilities (CVE-2014-0224, CVE-2014-0221, CVE-2

IBM notice: The page you requested cannot be displayed

IBM SDK for Node.js 1.1.0.4 for use by the Cordova tools

Security Advisory SA59126 - Huawei Multiple Products Multiple OpenSSL Vulnerabilities - Secunia

IBM Security Bulletin: Tivoli Management Framework is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, (

Security Advisory SA59189 - Blue Coat IntelligenceCenter OpenSSL Multiple Vulnerabilities - Secunia

IBM Support

SecurityFocus

Bug 1103598 – CVE-2014-0195 openssl: Buffer overflow via DTLS invalid fragment

Security Advisory SA58883 - F5 Multiple Products OpenSSL "dtls1_reassemble_fragment()" Buffer Overflow Vulnerability - Secuni

www.blackberry.com/btsc/KB36051

Security Advisory SA61254 - IBM InfoSphere Guardium Database Activity Monitor Multiple Vulnerabilities - Secunia

Security Advisory SA59491 - BlackBerry OS OpenSSL Multiple Vulnerabilities - Secunia

fsc-2014-6 | F-Secure Labs

[SECURITY] Fedora 20 Update: openssl-1.0.1e-39.fc20

Security Advisory SA58939 - IBM SmartCloud Orchestrator OpenSSL Multiple Vulnerabilities - Secunia

IBM Security Bulletin: IBM Tivoli Network Manager IP Edition V39 Fix Pack 4 HTTPS support for Perl Collector install is affected by the followi

Oracle Critical Patch Update - October 2017

IBM Support

VMSA-2014-0006.11 | United States

Security Advisory SA59364 - HP-UX update for OpenSSL - Secunia

Once Bled, Twice Shy (OpenSSL: CVE-2014-0195) - HP Enterprise Business Community

Security Advisory SA59306 - IBM i OpenSSL Multiple Vulnerabilities - Secunia

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)

590349 Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

591311 Bosch Rexroth RBA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)