CVE-2014-0076

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-0076
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-25 13:25:00 UTC
Updated	2023-02-13 00:31:00 UTC
Description	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a cc

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	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All

Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	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	0.9.6i	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	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	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	0.9.8m	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	0.9.8y	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	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	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	0.9.6i	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	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	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	0.9.8m	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	0.9.8y	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	All	All	All	All

References

Reference

Security Advisory SA59040 - Cisco AnyConnect VPN Client OpenSSL Multiple Vulnerabilities - Secunia

openSUSE-SU-2014:0480-1: moderate: openssl: fix for ECDSA side channel a

'[security bulletin] HPSBGN03050 rev.1 - HP IceWall SSO Dfw and HP IceWall MCRP running OpenSSL, Remo' - MARC

Mageia Advisory: MGASA-2014-0165 - Updated openssl package fix two security vulnerabilities

Security Advisory SA59162 - McAfee Multiple Products OpenSSL Multiple Vulnerabilities - Secunia

Support | OpenSSL Security Advisory (05 June 2014) and Open Enterprise Server 2 SP3.

OpenSSL CVE-2014-0076 Information Disclosure Weakness

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

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

About the security content of OS X Mavericks v10.9.5 and Security Update 2014-004 - Apple Support

505278 – (CVE-2014-0076) <dev-libs/openssl-{1.0.0l,1.0.1g}: ECDSA Nonces Recovery Weakness (CVE-2014-0076)

Security Advisory SA59514 - HP System Management Homepage 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

Security Advisory SA59655 - IBM SmartCloud Provisioning for IBM Provided Software Virtual Appliance OpenSSL Multiple Vulnerabilities - Se

IBM Security Bulletin: IBM Security Access Manager for Mobile and IBM Security Access Manager for Web appliances are affected by the follc

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

Support | OpenSSL Security Advisory (05 June 2014) and Open Enterprise Server 11 SP1.

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

Security Advisory SA59264 - Cisco WebEx Meetings Server / Unified Communications Manager OpenSSL Multiple Vulnerabilities - Secunia

Security Advisory SA59175 - HP OpenVMS update for SSL - Secunia

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

IBM notice: The page you requested cannot be displayed

Security Advisory SA59374 - Cisco IOS XE OpenSSL Multiple Vulnerabilities - Secunia

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

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

Security Advisory SA59438 - IBM Security Access Manager for Web / Security Access Manager for Mobile 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

IBM Security Bulletin: IBM Worklight is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-3470 and CVE-2014-00

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

Oracle Critical Patch Update - January 2015

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

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
Document Display | HPE Support Center
Security Advisory SA59495 - Novell Open Enterprise Server OpenSSL Multiple Vulnerabilities - Secunia
Cryptology ePrint Archive: Report 2014/140
Security Advisory SA59490 - HP Version Control Agent OpenSSL Multiple Vulnerabilities - Secunia
Support / Security / Advisories / / MDVSA-2015:062 | Mandriva
Security Advisory SA58492 - Cisco Multiple Products OpenSSL Two Vulnerabilities - Secunia
Access Denied
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
'[security bulletin] HPSBOV03047 rev.1 - HP OpenVMS running OpenSSL, Remote Denial of Service (DoS), ' - MARC
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products
IBM Security Bulletin: OpenSSL vulnerability in current release of the IBM® SDK for Node.js™ - United States
IBM notice: The page you requested cannot be displayed
www.openssl.org/news/secadv_20140605.txt
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 Advisory SA58727 - IBM SDK for Node.js OpenSSL ECDSA Nonces Recovery Weakness - Secunia
'[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
IBM Security Bulletin: SmartCloud Orchestrator is affected by the following OpenSSL vulnerabilities (CVE-2014-0224, CVE-2014-0221, CVE-2
IBM Security Bulletin: Tivoli Management Framework is affected by the following OpenSSL vulnerabilities: CVE-2014-0224, CVE-2014-0221, C
Support / Security / Advisories / / MDVSA-2014:067 | Mandriva
USN-2165-1: OpenSSL vulnerabilities | Ubuntu
Security Advisory SA58939 - IBM SmartCloud Orchestrator OpenSSL Multiple Vulnerabilities - Secunia
Security Advisory SA59445 - IBM Worklight OpenSSL Security Issue and Vulnerability - Secunia
Oracle Critical Patch Update - October 2017
IBM Security Bulletin: Potential Security Vulnerabilities fixed in IBM WebSphere Application Server 8.0.0.9 - United States
Security Advisory SA59364 - HP-UX update for OpenSSL - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

Legacy QID Mappings

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

591350 General Electric D20MX Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (PRSN-0006)

CVE.report and Source URL Uptime Status status.cve.report