CVE-2016-0800

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-0800
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-01 20:59:00 UTC
Updated	2022-12-13 12:15:00 UTC
Description	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to se

Risk And Classification

Problem Types: CWE-310 | CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All
Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	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	1.0.1n	All	All	All
Application	Openssl	Openssl	1.0.1o	All	All	All
Application	Openssl	Openssl	1.0.1p	All	All	All

Application	Openssl	Openssl	1.0.1q	All	All	All
Application	Openssl	Openssl	1.0.1r	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2e	All	All	All
Application	Openssl	Openssl	1.0.2f	All	All	All
Application	Pulsesecure	Client	-	All	All	All
Application	Pulsesecure	Client	-	All	All	All
Application	Pulsesecure	Steel Belted Radius	-	All	All	All
Application	Pulsesecure	Steel Belted Radius	-	All	All	All

References

Reference
Oracle Solaris Bulletin - April 2016
Oracle Critical Patch Update Advisory - April 2016
Knowledge Center
Document Display | HPE Support Center
[security-announce] openSUSE-SU-2016:0637-1: important: Security update
cert-portal.siemens.com/productcert/pdf/ssa-623229.pdf
[security-announce] SUSE-SU-2016:0617-1: important: Security update for
Oracle Critical Patch Update - July 2016
Siemens Industrial Products DROWN Vulnerability | ICS-CERT
[security-announce] openSUSE-SU-2016:0720-1: important: Security update
HPE Support document - HPE Support Center
HPE Support document - HPE Support Center
[security-announce] openSUSE-SU-2016:0627-1: important: Security update
[security-announce] SUSE-SU-2016:0624-1: important: Security update for
[security-announce] SUSE-SU-2016:0620-1: important: Security update for
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities
Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800) - Juniper Networks

OpenSSL Flaws Let Remote Users Deny Service and Decrypt TLS Sessions in Certain Cases - SecurityTracker

CVE-2016-0800 SSLv2 Vulnerability in Multiple NetApp Products | NetApp Product Security

OpenSSL: Multiple vulnerabilities (GLSA 201603-15) — Gentoo Security

HPE Support document - HPE Support Center

www.openssl.org/news/secadv/20160301.txt

DROWN Attack

Oracle Critical Patch Update - January 2018

[security-announce] SUSE-SU-2016:1057-1: important: Security update for

'[security bulletin] HPSBMU03573 rev.1 - HPE System Management Homepage (SMH), Remote Disclosure of I' - MARC

Siemens

Citrix XenServer Security Update for CVE-2016-0800

Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2016

Arista - Security Advisory 0018

OpenSSL DROWN Attack CVE-2016-0800 Security Bypass Vulnerability

DROWN - Cross-protocol attack on TLS using SSLv2 (CVE-2016-0800) - Red Hat Customer Portal

[security-announce] openSUSE-SU-2016:0638-1: important: Security update

[security-announce] SUSE-SU-2016:0678-1: important: Security update for

'[security bulletin] HPSBMU03575 rev.1 - HP Smart Update Manager (SUM), Remote Denial of Service (DoS' - MARC

Document Display | HPE Support Center

[security-announce] openSUSE-SU-2016:0628-1: important: Security update

[security-announce] SUSE-SU-2016:0631-1: important: Security update for

Document Display | HPE Support Center

[security-announce] openSUSE-SU-2016:1241-1: important: Security update

Oracle VM Server for x86 Bulletin - July 2016

Document Display | HPE Support Center

HPE Support document - HPE Support Center

[security-announce] SUSE-SU-2016:0641-1: important: Security update for

Security Advisory - OpenSSL DROWN Security Vulnerability

Document Display | HPE Support Center

StruxureWare Data Center Operation Software Vulnerability Fixes - User Assistance for StruxureWare Data Center Operation 8 - Help Center

Document Display | HPE Support Center

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

Oracle Linux Bulletin - January 2016

FreeBSD-SA-16:12

Document Display | HPE Support Center

[security-announce] SUSE-SU-2016:0621-1: important: Security update for
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates
Public KB - SA40168 - [Pulse Secure] March 1st 2016 OpenSSL Security Advisory
[security-announce] openSUSE-SU-2016:0640-1: important: Security update
Document Display | HPE Support Center
Vulnerability Note VU#583776 - Network traffic encrypted using RSA-based SSL certificates over SSLv2 may be decrypted by the DROWN at
Document Display | HPE Support Center
[security-announce] openSUSE-SU-2016:1239-1: important: Security update
Red Hat Customer Portal
'[security bulletin] HPSBGN03569 rev.1 - HPE OneView for VMware vCenter (OV4VC), Remote Disclosure of' - MARC
Oracle Solaris Bulletin - January 2016
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 378509 Splunk Enterprise Multiple Vulnerabilities (SP-CAAAPKV)
- 591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)
- 591286 Siemens SCALANCE DROWN (Decrypting Rivest Shamir Adleman (RSA) with Obsolete and Weakened eNcryption) Vulnerability (ICSA-16-103-03C, SSA-623229)
- 591311 Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)