CVE-2021-3450

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3450
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-25 15:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Freebsd	Freebsd	12.2	-	All	All
Operating System	Freebsd	Freebsd	12.2	p1	All	All
Operating System	Freebsd	Freebsd	12.2	p2	All	All
Application	Mcafee	Web Gateway	10.1.1	All	All	All
Application	Mcafee	Web Gateway	8.2.19	All	All	All
Application	Mcafee	Web Gateway	9.2.10	All	All	All
Application	Mcafee	Web Gateway Cloud Service	10.1.1	All	All	All
Application	Mcafee	Web Gateway Cloud Service	8.2.19	All	All	All
Application	Mcafee	Web Gateway Cloud Service	9.2.10	All	All	All
Application	Netapp	Cloud Volumes Ontap Mediator	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Hardware	Netapp	Santricity Smi-s Provider	-	All	All	All
Operating System	Netapp	Santricity Smi-s Provider Firmware	-	All	All	All
Hardware	Netapp	Storagegrid	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All

Operating System	Netapp	Storagegrid Firmware	-	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Oracle	Commerce Guided Search	11.3.2	All	All	All
Application	Oracle	Enterprise Manager For Storage Management	13.4.0.0	All	All	All
Application	Oracle	Graalvm	19.3.5	All	All	All
Application	Oracle	Graalvm	20.3.1.2	All	All	All
Application	Oracle	Graalvm	21.0.0.2	All	All	All
Application	Oracle	Jd Edwards Enterpriseone Tools	All	All	All	All
Application	Oracle	Jd Edwards World Security	a9.4	All	All	All
Application	Oracle	Mysql Connectors	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Server	All	All	All	All
Application	Oracle	Mysql Server	All	All	All	All
Application	Oracle	Mysql Workbench	All	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	All	All	All	All
Application	Oracle	Secure Backup	All	All	All	All
Application	Oracle	Secure Global Desktop	5.6	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	14.1.1.0.0	All	All	All
Application	Sonicwall	Capture Client	All	All	All	All
Application	Sonicwall	Email Security	All	All	All	All
Hardware	Sonicwall	Sma100	-	All	All	All
Operating System	Sonicwall	Sma100 Firmware	All	All	All	All
Operating System	Sonicwall	Sonicos	All	All	All	All
Application	Tenable	Nessus	All	All	All	All
Application	Tenable	Nessus Agent	All	All	All	All
Application	Tenable	Nessus Network Monitor	5.11.0	All	All	All
Application	Tenable	Nessus Network Monitor	5.11.1	All	All	All
Application	Tenable	Nessus Network Monitor	5.12.0	All	All	All
Application	Tenable	Nessus Network Monitor	5.12.1	All	All	All
Application	Tenable	Nessus Network Monitor	5.13.0	All	All	All
Operating System	Windriver	Linux	-	All	All	All
Operating System	Windriver	Linux	17.0	All	All	All
Operating System	Windriver	Linux	18.0	All	All	All

Operating System	Windriver	Linux	19.0	All	All	All

References

Reference
[SECURITY] Fedora 34 Update: openssl-1.1.1k-1.fc34 - package-announce - Fedora Mailing-Lists
git.openssl.org Git - openssl.git/commitdiff
Public KB - SA44845 - OpenSSL Security Advisory CVE-2021-3450
OpenSSL Security Advisory
Oracle Critical Patch Update Advisory - April 2022
March 2021 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security
[R1] Nessus Agent 8.2.4 Fixes Multiple Vulnerabilities - Security Advisory | Tenable®
Oracle Critical Patch Update Advisory - July 2021
www.openssl.org/news/secadv/20210325.txt
OpenSSL: Multiple vulnerabilities (GLSA 202103-03) — Gentoo security
Oracle Critical Patch Update Advisory - October 2021
[R1] Nessus Network Monitor 5.13.1 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®
git.openssl.org Git - openssl.git/commitdiff
security.FreeBSD.org/advisories/FreeBSD-SA-21:07.openssl.asc
McAfee Security Bulletin - Status and updates for OpenSSL vulnerabilities (CVE-2021-3450 and 2021-3449)
cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf
oss-security - Re: OpenSSL 1.1.1 CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT, CVE-2021-3449 NULL pc
Security Advisory
[R1] Nessus 8.13.2 Fixes Multiple Third-party Vulnerabilities - Security Advisory | Tenable®
oss-security - OpenSSL 1.1.1 CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT, CVE-2021-3449 NULL pointe
oss-security - Re: OpenSSL 1.1.1 CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT, CVE-2021-3449 NULL pc
[SECURITY] Fedora 34 Update: openssl-1.1.1k-1.fc34 - package-announce - Fedora Mailing-Lists
Oracle Critical Patch Update Advisory - July 2022
Oracle Critical Patch Update Advisory - April 2021
oss-security - Re: OpenSSL 1.1.1 CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT, CVE-2021-3449 NULL pc
Multiple Vulnerabilities in OpenSSL Affecting Cisco Products: March 2021
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Benjamin Kaduk (Akamai), Xiang Ding (Akamai), others at Akamai

Legacy QID Mappings

159128 Oracle Enterprise Linux Security Update for openssl (ELSA-2021-1024)

159138 Oracle Enterprise Linux Security Update for openssl (ELSA-2021-9151)

179935 Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2021-3450)

239185 Red Hat Update for openssl (RHSA-2021:1024)

239247 Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP7 (RHSA-2021:1199)

239730 Red Hat Update for red hat jboss web server 5.4.2 (RHSA-2021:1195)

239739 Red Hat Update for red hat jboss web server 3.1 service pack 12 (RHSA-2021:1202)

281398 Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2021-cbf14ab8f9)

296053 Oracle Solaris 11.4 Support Repository Update (SRU) 35.94.4 Missing (CPUJUL2021)

296059 Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)

316994 Cisco Internetwork Operating System (IOS-XE) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)

316995 Cisco Nexus Operating System (NX-OS) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)

316996 Cisco Web Security Appliance Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)

352258 Amazon Linux Security Advisory for openssl11: ALAS2-2021-1622

357333 Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502

375520 Mysql Workbench Critical Patch Update April 2021

375559 Python Open Secure Sockets Layer (OpenSSL) Library Vulnerability

375656 Tenable Nessus Agent Multiple Vulnerabilities (TNS-2021-08)

375720 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJUL2021)

377109 Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2021:0021)

38837 OpenSSL Security Update (OpenSSL Security Advisory 20210325)

500498 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500566 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

500765 Alpine Linux Security Update for openssl

501165 Alpine Linux Security Update for openssl

501984 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)

502903 Alpine Linux Security Update for openssl1.1-compat

504257 Alpine Linux Security Update for openssl

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

690068 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (38a4a043-e937-11eb-9b84-d4c9ef517024)

690183 Free Berkeley Software Distribution (FreeBSD) Security Update for node.js (c0c1834c-9761-11eb-acfd-0022489ad614)

690185 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (5a668ab3-8d86-11eb-b8d6-d4c9ef517024)

710009 Gentoo Linux OpenSSL Multiple Vulnerabilities (GLSA 202103-03)

730135 Cisco Prime Infrastructure Denial of Service (DoS) Vulnerability in Open Secure Sockets Layer (OpenSSL) Affecting Cisco Products (cisco-sa-openssl-2021-GHY28dJd)

730228 McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-3611)

750833 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:2327-1)

750837 SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2021:2353-1)

750840 OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:2353-1)

750858 OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:1061-1)

750859 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1059-1)

91783 IBM Integration Bus and IBM App Connect Enterprise Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (6466315)

91784 IBM Integration Bus and IBM App Connect Enterprise Node.js Multiple Vulnerabilities (6467639)

91822 Microsoft Visual Studio Security Update for October 2021

940369 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2021:1024)

960860 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2021:1024)