



CVE-2022-3602

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

Summary

CVE	CVE-2022-3602
State	PUBLIC
Assigner	openssl-security@openssl.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-01 18:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occ

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	26	All	All	All
Operating System	Fedoraproject	Fedora	27	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	18.12.0	All	All	All
Application	Nodejs	Node.js	19.0.0	All	All	All
Application	Openssl	Openssl	All	All	All	All

References

Reference

www.openssl.org/news/secadv/20221101.txt

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Ove

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Ove

[SECURITY] Fedora 36 Update: openssl-3.0.5-2.fc36 - package-announce - Fedora Mailing-Lists

git.openssl.org Git - openssl.git/commitdiff

Security Advisory

20221028 Vulnerabilities in OpenSSL Affecting Cisco Products: November 2022

OpenSSL: Multiple Vulnerabilities (GLSA 202211-01) — Gentoo security

VU#794340 - OpenSSL 3.0.0 to 3.0.6 decodes some punycode email addresses in X.509 certificates improperly

oss-security - Re: Fwd: Node.js security updates for all active release lines, November 2022

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

[SECURITY] Fedora 37 Update: openssl-3.0.5-3.fc37 - package-announce - Fedora Mailing-Lists

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

OpenSSL Security Advisory 20221101 ≈ Packet Storm

git.openssl.org Git - openssl.git/commitdiff

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

November 2022 OpenSSL Vulnerabilities in NetApp Products | NetApp Product Security

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

[SECURITY] Fedora 36 Update: openssl-3.0.5-2.fc36 - package-announce - Fedora Mailing-Lists

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

[SECURITY] Fedora 37 Update: openssl-3.0.5-3.fc37 - package-announce - Fedora Mailing-Lists

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

oss-security - Re: Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow

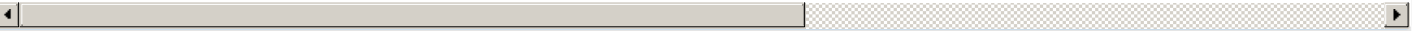
oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Ove

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Ove

oss-security - Re: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Ove

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160191](#) Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-7288)

[160192](#) Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-9968)

[160258](#) Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2022-10004)

[183501](#) Debian Security Update for Open Secure Sockets Layer (OpenSSL) (CVE-2022-3602)

[199012](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[199113](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[199114](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[199115](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[199116](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[199117](#) Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-5710-1)

[240798](#) Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2022:7288)

[283270](#) Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-502f096dce)

[283442](#) Fedora Security Update for Open Secure Sockets Layer (OpenSSL) (FEDORA-2022-0f1d2e0537)

[296086](#) Oracle Solaris 11.4 Support Repository Update (SRU) 51.132.1 Missing (CPUOCT2022)

[296098](#) Oracle Solaris 11.4 Support Repository Update (SRU) 52.132.2 Missing (CPUOCT2022)

[330128](#) IBM AIX Multiple Vulnerabilities in Open Secure Sockets Layer (OpenSSL) (openssl_advisory37)

[354102](#) Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-157

[354404](#) Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2022-2022-157

[355250](#) Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-051

[355273](#) Amazon Linux Security Advisory for nodejs : ALAS2023-2023-084

[377733](#) Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Buffer Overflow Vulnerability (Scan Utility)

[377981](#) Node.js Multiple Vulnerabilities (November 2022)

377001 Node.js Multiple Vulnerabilities (November 2022)
377934 Node.js Multiple Vulnerabilities (November 2022)
38879 Open Secure Sockets Layer (OpenSSL) Less Than 3.0.7 Buffer Overflow Vulnerability
43945 FortiOS - Unauthorized Command Execution Vulnerability (FG-IR-22-419)
502587 Alpine Linux Security Update for Open Secure Sockets Layer3 (OpenSSL3)
502747 Alpine Linux Security Update for nodejs
502755 Alpine Linux Security Update for openssl
503688 Alpine Linux Security Update for openssl3
520001 Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (CVE-2022-3602, CVE-2022-3786)
591335 Hitachi Energy PCU400 Reliance on Uncontrolled Component Multiple Vulnerabilities (ICSA-23-019-01, 8DBD 000137)
690972 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (0844671c-5a09-11ed-856e-d4c9ef517024)
710678 Gentoo Linux Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (GLSA 202211-01)
752752 SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL-3) (SUSE-SU-2022:3843-1)
940723 AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2022:7288)
960515 Rocky Linux Security Update for Open Secure Sockets Layer (OpenSSL) (RLSA-2022:7288)

© [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](#)