



CVE-2021-27918

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

Summary

CVE	CVE-2021-27918
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-11 00:15:00 UTC
Updated	2022-12-13 16:28:00 UTC
Description	encoding/xml in Go before 1.15.9 and 1.16.x before 1.16.1 has an infinite loop if a custom TokenReader (for xml.NewToken

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All

References

Reference	Source	Link	Tags
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org	
[security] Go 1.16.1 and Go 1.15.9 are released	MISC	groups.google.com	Mailing List, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159237](#) Oracle Enterprise Linux Security Update for olcne (ELSA-2021-9267)
- [159238](#) Oracle Enterprise Linux Security Update for olcne (ELSA-2021-9268)
- [159347](#) Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-3076)
- [174832](#) SUSE Enterprise Linux Security update for go1.15 (SUSE-SU-2021:0938-1)

174835 SUSE Enterprise Linux Security update for go1.16 (SUSE-SU-2021:0937-1)
174851 SUSE Enterprise Linux Security update for go1.15 (SUSE-SU-2021:0938-1)
174854 SUSE Enterprise Linux Security update for go1.16 (SUSE-SU-2021:0937-1)
179711 Debian Security Update for golang-1.15 (CVE-2021-27918)
239549 Red Hat Update for go-toolset:rhel8 (RHSA-2021:3076)
354041 Amazon Linux Security Advisory for golang : ALAS2-2022-1830
377560 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0060)
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
501568 Alpine Linux Security Update for go
501857 Alpine Linux Security Update for go
670419 EulerOS Security Update for golang (EulerOS-SA-2021-1980)
670439 EulerOS Security Update for golang (EulerOS-SA-2021-2061)
670450 EulerOS Security Update for golang (EulerOS-SA-2021-2050)
670459 EulerOS Security Update for golang (EulerOS-SA-2021-2217)
690234 Free Berkeley Software Distribution (FreeBSD) Security Update for go (72709326-81f7-11eb-950a-00155d646401)
710584 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
750292 OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:0480-1)
900159 CBL-Mariner Linux Security Update for golang 1.15.7
903202 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3968)
907749 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (3968-1)
940126 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:3076)
960708 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:3076)

© [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](#)