



CVE-2021-44717

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

Summary

CVE	CVE-2021-44717
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-01 05:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network co

Risk And Classification

Problem Types: CWE-404

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Golang	Go	All	All	All	All
Operating System	Opengroup	Unix	-	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3395-1] golang-1.11 security update	MLIST	lists.debian.org	
cert-portal.siemens.com/productcert/pdf/ssa-744259.pdf	MISC	cert-portal.siemens.com	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org	
[security] Go 1.17.5 and Go 1.16.12 are released	CONFIRM	groups.google.com	
[SECURITY] [DLA 2892-1] golang-1.7 security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2891-1] golang-1.8 security update	MLIST	lists.debian.org	
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 OID Mappings

159553 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-5160)
179017 Debian Security Update for golang-1.8 (DLA 2891-1)
179018 Debian Security Update for golang-1.7 (DLA 2892-1)
179594 Debian Security Update for golang-1.15 (CVE-2021-44717)
181743 Debian Security Update for golang-1.11 (DLA 3395-1)
239964 Red Hat Update for go-toolset:rhel8 (RHSA-2021:5160)
240138 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)
240161 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:0927)
282205 Fedora Security Update for golang (FEDORA-2021-29943703de)
282206 Fedora Security Update for golang (FEDORA-2021-6fdc5ea304)
353263 Amazon Linux Security Advisory for golang : ALAS2-2022-1776
353275 Amazon Linux Security Advisory for golang : ALAS-2022-1583
353977 Amazon Linux Security Advisory for golang : ALAS2-2022-1811
354488 Amazon Linux Security Advisory for golang : ALAS2022-2022-009
354527 Amazon Linux Security Advisory for golang : ALAS2022-2022-193
354566 Amazon Linux Security Advisory for golang : ALAS-2022-193
355212 Amazon Linux Security Advisory for golang : ALAS2023-2023-048
356304 Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-002
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
502093 Alpine Linux Security Update for go
502126 Alpine Linux Security Update for nomad
502297 Alpine Linux Security Update for go
502316 Alpine Linux Security Update for nomad
671452 EulerOS Security Update for golang (EulerOS-SA-2022-1449)
671472 EulerOS Security Update for golang (EulerOS-SA-2022-1428)
671491 EulerOS Security Update for golang (EulerOS-SA-2022-1506)
671527 EulerOS Security Update for golang (EulerOS-SA-2022-1487)
690735 Free Berkeley Software Distribution (FreeBSD) Security Update for go (720505fe-593f-11ec-9ba8-002324b2fba8)

710584 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
751547 SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2021:4169-1)
751549 SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2021:4186-1)
751553 OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:4169-1)
751554 OpenSUSE Security Update for go1.17 (openSUSE-SU-2021:4186-1)
751559 OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1626-1)
753532 OpenSUSE Security Update for aptainer (openSUSE-SU-2023:0018-1)
770138 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)
770140 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:0927)
940411 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:5160)
960760 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:5160)

© [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](#)