



CVE-2021-36221

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

Summary

CVE	CVE-2021-36221
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-08 06:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	Go before 1.15.15 and 1.16.x before 1.16.7 has a race condition that can lead to a net/http/httputil ReverseProxy panic upon

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Golang	Go	All	All	All	All
Application	Oracle	Timesten In-memory Database	All	All	All	All
Hardware	Siemens	Scalance Lpe9403	-	All	All	All
Operating System	Siemens	Scalance Lpe9403 Firmware	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3395-1] golang-1.11 security update	MLIST	lists.debian.org
Google Gruplar'a yönlendiriliyorsunuz		groups.google.com
Go 1.16.7 and Go 1.15.15 are released	MISC	groups.google.com
[SECURITY] Fedora 33 Update: golang-1.15.15-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com
cert-portal.siemens.com/productcert/pdf/ssa-222547.pdf	CONFIRM	cert-portal.siemens.com

Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org
[security] Go 1.16.6 and Go 1.15.14 pre-announcement	MISC	groups.google.com
Google Gruplar'a yönlendiriliyorsunuz	MISC	groups.google.com
[SECURITY] Fedora 34 Update: golang-1.16.8-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 33 Update: golang-1.15.15-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: golang-1.16.8-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 2892-1] golang-1.7 security update	MLIST	lists.debian.org
[SECURITY] Fedora 34 Update: golang-1.16.8-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: golang-1.16.8-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 2891-1] golang-1.8 security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160233 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2022-7457)
179017 Debian Security Update for golang-1.8 (DLA 2891-1)
179018 Debian Security Update for golang-1.7 (DLA 2892-1)
180333 Debian Security Update for golang-1.15 (CVE-2021-36221)
181743 Debian Security Update for golang-1.11 (DLA 3395-1)
239803 Red Hat Update for go-toolset:rhel8 security (RHSA-2021:4156)
240106 Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)
240829 Red Hat Update for container-tools:rhel8 security (RHSA-2022:7457)
281906 Fedora Security Update for golang (FEDORA-2021-38b51d9fd3)
281921 Fedora Security Update for golang (FEDORA-2021-6a3024b3fd)
296063 Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022)
352848 Amazon Linux Security Advisory for golang: ALAS-2021-1538
353094 Amazon Linux Security Advisory for golang : AL2012-2021-355
354041 Amazon Linux Security Advisory for golang : ALAS2-2022-1830
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
501572 Alpine Linux Security Update for go

501861	Alpine Linux Security Update for go
590976	Siemens SCALANCE LPE9403 Third-Party Multiple Vulnerabilities (ICSA-22-167-09) (SSA-222547)
671161	EulerOS Security Update for golang (EulerOS-SA-2021-2802)
671187	EulerOS Security Update for golang (EulerOS-SA-2021-2930)
671209	EulerOS Security Update for golang (EulerOS-SA-2022-1027)
671229	EulerOS Security Update for golang (EulerOS-SA-2022-1007)
671286	EulerOS Security Update for golang (EulerOS-SA-2022-1254)
671311	EulerOS Security Update for golang (EulerOS-SA-2022-1242)
690066	Free Berkeley Software Distribution (FreeBSD) Security Update for go (880552c4-f63f-11eb-9d56-7186043316e9)
710584	Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
750986	SUSE Enterprise Linux Security Update for go1.15 (SUSE-SU-2021:2787-1)
751012	OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:2787-1)
751017	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:2788-1)
751041	OpenSUSE Security Update for go1.16 (openSUSE-SU-2021:1199-1)
751066	OpenSUSE Security Update for go1.15 (openSUSE-SU-2021:1207-1)
770136	Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)
900310	CBL-Mariner Linux Security Update for golang 1.15.13
903311	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (5296)
907746	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (5296-1)
940216	AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:4156)
960743	Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:4156)

© [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](#)