



CVE-2021-29923

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

Summary

CVE	CVE-2021-29923
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-07 17:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	Go before 1.17 does not properly consider extraneous zero characters at the beginning of an IP address octet, which (in so

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Golang	Go	All	All	All	All
Application	Oracle	Timesten In-memory Database	All	All	All	All

References

Reference	Source	Link
go-review.googlesource.com/c/go/+325829	MISC	go-review.googlesource.com/c/go/+325829
net · pkg.go.dev	MISC	golang.org
security/SICK-2021-016.md at master · sickcodes/security · GitHub	MISC	github.com
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com
net: limit the size of ParseIP input? · Issue #43389 · golang/go · GitHub	MISC	github.com
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 36 Update: golang-1.18~rc1-2.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 36 Update: golang-1.18~rc1-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
defcon.org/html/defcon-29/dc-29-speakers.html	MISC	defcon.org
net: reject leading zeros in IP address parsers [freeze exception] · Issue #30999 · golang/go · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159397](#) Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2021-3585)

[239647](#) Red Hat Update for go-toolset:rhel8 (RHSA-2021:3585)

[240023](#) Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0237)

[240030](#) Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0260)

[240106](#) Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)

[240171](#) Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0988)

[240173](#) Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0998)

[240177](#) Red Hat Update for OpenStack Platform 16.1 (RHSA-2022:0989)

[240183](#) Red Hat Update for OpenStack Platform 16.2 (RHSA-2022:0997)

[375831](#) Golang Improper Input Validation Of Octal Literals Vulnerability

[377556](#) Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2021:0069)

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[502089](#) Alpine Linux Security Update for go

[503185](#) Alpine Linux Security Update for go

[506078](#) Alpine Linux Security Update for go

[671032](#) EulerOS Security Update for golang (EulerOS-SA-2021-2633)

[671038](#) EulerOS Security Update for golang (EulerOS-SA-2021-2661)

[671209](#) EulerOS Security Update for golang (EulerOS-SA-2022-1027)

[671229](#) EulerOS Security Update for golang (EulerOS-SA-2022-1007)

[710584](#) Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)

[770136](#) Red Hat OpenShift Container Platform 4.9 Security Update (RHSA-2022:0557)

[900300](#) CBL-Mariner Linux Security Update for golang 1.15.13

[900322](#) CBL-Mariner Linux Security Update for golang 1.16.7

[903052](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (5242)

[907745](#) CBL-Mariner Linux Security Update for golang 1.16.7 (5010-1)

[907745](#) Common Base Linux Mariner (CBL-Mariner) Security Update for gojang (5242-1)

[940338](#) AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2021:3585)

[960681](#) Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2021:3585)

© [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](#)