



CVE-2022-32149

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

Summary

CVE	CVE-2022-32149
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-14 15:15:00 UTC
Updated	2022-10-18 17:41:00 UTC
Description	An attacker may cause a denial of service by crafting an Accept-Language header which ParseAcceptLanguage will take si

Risk And Classification

Problem Types: CWE-772

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
GO-2022-1059 - Go Packages	MISC	pkg.go.de
x/text/language: ParseAcceptLanguage takes a long time to parse complex tags · Issue #56152 · golang/go · GitHub	MISC	go.dev
go.dev/cl/442235	MISC	go.dev
[security] Vulnerability in golang.org/x/text/language	MISC	groups.gc
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184247 Debian Security Update for golang-golang-x-text (CVE-2022-32149)

199182 Ubuntu Security Notification for Go Text Vulnerabilities (USN-5873-1)

041717 Debian Security Update for golang-golang-x-text (CVE-2022-32149)

241747 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3613)
357051 Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2024-035
357058 Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2024-035
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
502841 Alpine Linux Security Update for docker-cli-compose
502856 Alpine Linux Security Update for gitea
505740 Alpine Linux Security Update for gitea
710660 Gentoo Linux Gitea Multiple Vulnerabilities (GLSA 202210-14)
754116 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:2578-1)
754978 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:3868-1)
754979 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:3867-1)
770197 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3613)
907624 Common Base Linux Mariner (CBL-Mariner) Security Update for kured (31972-1)
907966 Common Base Linux Mariner (CBL-Mariner) Security Update for sriov-network-device-plugin (33643-1)
908029 Common Base Linux Mariner (CBL-Mariner) Security Update for node-problem-detector (33628)

© [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](#)