CVE-2022-41725

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-41725
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-28 18:15:00 UTC
Updated	2023-11-25 11:15:00 UTC
Description	A denial of service is possible from excessive resource consumption in net/http and mime/multipart. Multipart form parsing v

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Application	Golang	Go	1.20.0	-	All	All
Application	Golang	Go	1.20.0	rc1	All	All
Application	Golang	Go	1.20.0	rc2	All	All
Application	Golang	Go	1.20.0	rc3	All	All

References

Reference	So
Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security	
GO-2023-1569 - Go Packages	MI
go.dev/cl/468124	MI
[security] Go 1.20.1 and Go 1.19.6 are released	MI
net/http, mime/multipart: denial of service from excessive resource consumption (CVE-2022-41725) · Issue #58006 · golang/go · GitHub	MI
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160699 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2023-3083)

161061 Oracle Enterprise Linux Security Update for skopeo (ELSA-2023-6363)

161062 Oracle Enterprise Linux Security Update for containernetworking-plugins (ELSA-2023-6402)

161063 Oracle Enterprise Linux Security Update for podman (ELSA-2023-6474)

161105 Oracle Enterprise Linux Security Update for buildah (ELSA-2023-6473)

161175 Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2023-6939)

161187 Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2023-6938)

182304 Debian Security Update for golang-1.19 (CVE-2022-41725)

199396 Ubuntu Security Notification for Go Vulnerabilities (USN-6140-1)

241473 Red Hat Update for go-toolset:rhel8 (RHSA-2023:3083)

241546 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:1325)

241582 Red Hat Update for OpenStack Platform 16.2 (RHSA-2023:3445)

241745 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)

242287 Red Hat Update for buildah (RHSA-2023:6473)

242288 Red Hat Update for toolbox (RHSA-2023:6346)

242299 Red Hat Update for containernetworking-plugins (RHSA-2023:6402)

242319 Red Hat Update for skopeo (RHSA-2023:6363)

242335 Red Hat Update for podman security (RHSA-2023:6474)

242365 Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5964)

242415 Red Hat Update for container-tools:rhel8 (RHSA-2023:6939)

242458 Red Hat Update for container-tools:4.0 (RHSA-2023:6938)

354890 Amazon Linux Security Advisory for golang : ALAS2-2023-2015

354901 Amazon Linux Security Advisory for golang : ALAS-2023-1731

355216 Amazon Linux Security Advisory for golang : ALAS2023-2023-175

355697 Amazon Linux Security Advisory for golang : ALAS2-2023-2163

355797 Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2023-026

355837 Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2023-029

356304 Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-002

379641 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)

502861 Alpine Linux Security Update for go

503186 Alpine Linux Security Update for go

506079 Alpine Linux Security Update for go

672934 EulerOS Security Update for golang (EulerOS-SA-2023-1822)

672950 EulerOS Security Update for golang (EulerOS-SA-2023-1804)

672974 EulerOS Security Update for golang (EulerOS-SA-2023-1844)

673009 EulerOS Security Update for golang (EulerOS-SA-2023-1869)

673123 EulerOS Security Update for golang (EulerOS-SA-2023-2292)

673132 EulerOS Security Update for golang (EulerOS-SA-2023-2268)

691061 Free Berkeley Software Distribution (FreeBSD) Security Update for go (3d73e384-ad1f-11ed-983c-83fe35862e3a)

710791 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)

753772 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:0733-1)

753836 SUSE Enterprise Linux Security Update for go1.18 (SUSE-SU-2023:0869-1)

753839 SUSE Enterprise Linux Security Update for container-suseconnect (SUSE-SU-2023:0871-1)

754047 SUSE Enterprise Linux Security Update for go1.18-openssl (SUSE-SU-2023:2312-1)

770186 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:1325)

770195 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)

905635 Common Base Linux Mariner (CBL-Mariner) Security Update for gcc (13717)

905637 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (13719)

905646 Common Base Linux Mariner (CBL-Mariner) Security Update for gcc (13729)

905647 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (13739)

905648 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (13732)

907046 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (13739-1)

907356 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (13732-1)

907744 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (13719-1)

907836 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (13732-2)

941076 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2023:3083)

941383 AlmaLinux Security Update for containernetworking-plugins (ALSA-2023:6402)

941386 AlmaLinux Security Update for buildah (ALSA-2023:6473)

941391 AlmaLinux Security Update for toolbox (ALSA-2023:6346)

941399 AlmaLinux Security Update for podman (ALSA-2023:6474)

941405 AlmaLinux Security Update for skopeo (ALSA-2023:6363)

941444 AlmaLinux Security Update for container-tools:4.0 (ALSA-2023:6938)

941481 AlmaLinux Security Update for container-tools:rhel8 (ALSA-2023:6939)

960933 Rocky Linux Security Update for go-toolset:Rocky (RLSA-2023:3083)

© 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 registred 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