



# CVE-2023-24534

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

## Summary

<b>CVE</b>	CVE-2023-24534
<b>State</b>	PUBLIC
<b>Assigner</b>	security@golang.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-06 16:15:00 UTC
<b>Updated</b>	2023-11-25 11:15:00 UTC
<b>Description</b>	HTTP and MIME header parsing can allocate large amounts of memory, even when parsing small inputs, potentially leading

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source
Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security	
April 2023 Golang Vulnerabilities in NetApp Products   NetApp Product Security	MISC
[security] Go 1.20.3 and Go 1.19.8 are released	MISC
GO-2023-1704 - Go Packages	MISC
go.dev/cl/481994	MISC
net/http, net/textproto: denial of service from excessive memory allocation (CVE-2023-24534) · Issue #58975 · golang/go · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

<a href="#">161062</a> Oracle Enterprise Linux Security Update for containernetworking-plugins (ELSA-2023-6402)
<a href="#">161063</a> Oracle Enterprise Linux Security Update for podman (ELSA-2023-6474)
<a href="#">161102</a> Oracle Enterprise Linux Security Update for grafana security and enhancement update (ELSA-2023-6420)
<a href="#">161105</a> Oracle Enterprise Linux Security Update for buildah (ELSA-2023-6473)
<a href="#">161175</a> Oracle Enterprise Linux Security Update for container-tools:ol8 (ELSA-2023-6939)
<a href="#">161187</a> Oracle Enterprise Linux Security Update for container-tools:4.0 (ELSA-2023-6938)
<a href="#">182296</a> Debian Security Update for golang-1.19 (CVE-2023-24534)
<a href="#">199304</a> Ubuntu Security Notification for Go Vulnerabilities (USN-6038-1)
<a href="#">199396</a> Ubuntu Security Notification for Go Vulnerabilities (USN-6140-1)
<a href="#">241582</a> Red Hat Update for OpenStack Platform 16.2 (RHSA-2023:3445)
<a href="#">241715</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3540)
<a href="#">241745</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)
<a href="#">241856</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)
<a href="#">241924</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4459)
<a href="#">242287</a> Red Hat Update for buildah (RHSA-2023:6473)
<a href="#">242288</a> Red Hat Update for toolbox (RHSA-2023:6346)
<a href="#">242299</a> Red Hat Update for containernetworking-plugins (RHSA-2023:6402)
<a href="#">242309</a> Red Hat Update for grafana (RHSA-2023:6420)
<a href="#">242319</a> Red Hat Update for skopeo (RHSA-2023:6363)
<a href="#">242335</a> Red Hat Update for podman security (RHSA-2023:6474)
<a href="#">242365</a> Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5964)
<a href="#">242415</a> Red Hat Update for container-tools:rhel8 (RHSA-2023:6939)
<a href="#">242458</a> Red Hat Update for container-tools:4.0 (RHSA-2023:6938)
<a href="#">354890</a> Amazon Linux Security Advisory for golang : ALAS2-2023-2015
<a href="#">354901</a> Amazon Linux Security Advisory for golang : ALAS-2023-1731
<a href="#">355089</a> Amazon Linux Security Advisory for golang : ALAS2-2023-2037
<a href="#">355216</a> Amazon Linux Security Advisory for golang : ALAS2023-2023-175
<a href="#">355797</a> Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2023-026

<a href="#">355837</a> Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2023-029
<a href="#">356180</a> Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-001
<a href="#">356503</a> Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001
<a href="#">379641</a> Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)
<a href="#">502863</a> Alpine Linux Security Update for go
<a href="#">502894</a> Alpine Linux Security Update for nomad
<a href="#">503188</a> Alpine Linux Security Update for go
<a href="#">503204</a> Alpine Linux Security Update for nomad
<a href="#">503271</a> Alpine Linux Security Update for traefik
<a href="#">506081</a> Alpine Linux Security Update for go
<a href="#">506263</a> Alpine Linux Security Update for traefik
<a href="#">673181</a> EulerOS Security Update for golang (EulerOS-SA-2023-2334)
<a href="#">673202</a> EulerOS Security Update for golang (EulerOS-SA-2023-2314)
<a href="#">673210</a> EulerOS Security Update for golang (EulerOS-SA-2023-2382)
<a href="#">673238</a> EulerOS Security Update for golang (EulerOS-SA-2023-2356)
<a href="#">673548</a> EulerOS Security Update for golang (EulerOS-SA-2023-2644)
<a href="#">673694</a> EulerOS Security Update for golang (EulerOS-SA-2023-2686)
<a href="#">691117</a> Free Berkeley Software Distribution (FreeBSD) Security Update for go (348ee234-d541-11ed-ad86-a134a566f1e6)
<a href="#">691126</a> Free Berkeley Software Distribution (FreeBSD) Security Update for traefik (02e51cb3-d7e4-11ed-9f7a-5404a68ad561)
<a href="#">710791</a> Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)
<a href="#">753895</a> SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:1792-1)
<a href="#">753976</a> SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:2127-1)
<a href="#">753977</a> SUSE Enterprise Linux Security Update for go1.20 (SUSE-SU-2023:2105-2)
<a href="#">770195</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)
<a href="#">770200</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)
<a href="#">770202</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4459)
<a href="#">907515</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (25990-1)
<a href="#">907873</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (25990-2)
<a href="#">907885</a> Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (26027-1)

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)
941404 AlmaLinux Security Update for grafana (ALSA-2023:6420)
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)

© [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](#)**