



# CVE-2023-24536

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

## Summary

<b>CVE</b>	CVE-2023-24536
<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>	Multipart form parsing can consume large amounts of CPU and memory when processing form inputs containing very large

## 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

## References

### Reference

- Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security  
go.dev/cl/482076
- April 2023 Golang Vulnerabilities in NetApp Products | NetApp Product Security  
go.dev/cl/482077
- [security] Go 1.20.3 and Go 1.19.8 are released  
go.dev/cl/482075
- GO-2023-1705 - Go Packages
- net/http, net/textproto, mime/multipart: denial of service from excessive resource consumption (CVE-2023-24536) · Issue #59153 · golang/go · CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[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)

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

[241715](#) Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3540)

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

[241856](#) Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)

[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

[356180](#) Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-001

[356503](#) Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001

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

[502863](#) Alpine Linux Security Update for go

503188 Alpine Linux Security Update for go
506081 Alpine Linux Security Update for go
673210 EulerOS Security Update for golang (EulerOS-SA-2023-2382)
673238 EulerOS Security Update for golang (EulerOS-SA-2023-2356)
673548 EulerOS Security Update for golang (EulerOS-SA-2023-2644)
673694 EulerOS Security Update for golang (EulerOS-SA-2023-2686)
691117 Free Berkeley Software Distribution (FreeBSD) Security Update for go (348ee234-d541-11ed-ad86-a134a566f1e6)
710791 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)
753895 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:1792-1)
753976 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:2127-1)
753977 SUSE Enterprise Linux Security Update for go1.20 (SUSE-SU-2023:2105-2)
770195 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)
770200 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)
907884 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (26028-1)
908056 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (37431-1)
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)
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](#)**