



CVE-2023-24538

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

Summary

CVE	CVE-2023-24538
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-06 16:15:00 UTC
Updated	2023-11-25 11:15:00 UTC
Description	Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected. Back

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security		security.gentoo.org
[security] Go 1.20.3 and Go 1.19.8 are released	MISC	groups.google.com
GO-2023-1703 - Go Packages	MISC	pkg.go.dev
go.dev/cl/482079	MISC	go.dev
html/template: backticks not treated as string delimiters (CVE-2023-24538) · Issue #59234 · golang/go · GitHub	MISC	go.dev
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)
182213 Debian Security Update for golang-1.19 (CVE-2023-24538)
199304 Ubuntu Security Notification for Go Vulnerabilities (USN-6038-1)
199396 Ubuntu Security Notification for Go Vulnerabilities (USN-6140-1)
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)
296100 Oracle Solaris 11.4 Support Repository Update (SRU) 58.144.3 Missing (CPUAPR2023)
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
356428 Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2-2023-2303

356458 Amazon Linux Security Advisory for amazon-ssm-agent : ALAS-2023-1866
356503 Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001
356521 Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2023-2023-388
356574 Amazon Linux Security Advisory for docker : ALAS2ECS-2023-019
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
673181 EulerOS Security Update for golang (EulerOS-SA-2023-2334)
673202 EulerOS Security Update for golang (EulerOS-SA-2023-2314)
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)
691156 Free Berkeley Software Distribution (FreeBSD) Security Update for grafana (0b85b1cd-e468-11ed-834b-6c3be5272acd)
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)
906880 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (25992-1)
907854 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (25992-2)
907897 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (25993-1)
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)

[941399](#) AlmaLinux Security Update for pcpmail (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](#)