



# CVE-2023-24540

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

## Summary

<b>CVE</b>	CVE-2023-24540
<b>State</b>	PUBLIC
<b>Assigner</b>	security@golang.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-11 16:15:00 UTC
<b>Updated</b>	2023-11-07 04:08:00 UTC
<b>Description</b>	Not all valid JavaScript whitespace characters are considered to be whitespace. Templates containing whitespace character

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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	Tags
GO-2023-1752 - Go Packages	MISC	<a href="https://pkg.go.dev">pkg.go.dev</a>	
html/template: improper handling of JavaScript whitespace · Issue #59721 · golang/go · GitHub	MISC	<a href="https://go.dev">go.dev</a>	
<a href="https://go.dev/cl/491616">go.dev/cl/491616</a>	MISC	<a href="https://go.dev">go.dev</a>	
[security] Go 1.20.4 and Go 1.19.9 are released	MISC	<a href="https://groups.google.com">groups.google.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

160702 Oracle Enterprise Linux Security Update for go-toolset and golang (ELSA-2023-3318)

160703 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2023-3319)

161001 Oracle Enterprise Linux Security Update for go-toolset:ol9 (ELSA-2023-3320)

<a href="#">161061</a> 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="#">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="#">199396</a> Ubuntu Security Notification for Go Vulnerabilities (USN-6140-1)
<a href="#">241559</a> Red Hat Update for go-toolset and golang (RHSA-2023:3318)
<a href="#">241560</a> Red Hat Update for go-toolset:rhel8 (RHSA-2023:3319)
<a href="#">241582</a> Red Hat Update for OpenStack Platform 16.2 (RHSA-2023:3445)
<a href="#">241623</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3366)
<a href="#">241687</a> Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3409)
<a href="#">241700</a> Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3545)
<a href="#">241745</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)
<a href="#">241775</a> Red Hat Update for red hat openshift enterprise (RHSA-2023:3910)
<a href="#">241776</a> Red Hat Update for red hat openshift enterprise (RHSA-2023:3914)
<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="#">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="#">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="#">296101</a> Oracle Solaris 11.4 Support Repository Update (SRU) 59.138.2 Missing (CPUJUL2023)
<a href="#">355425</a> Amazon Linux Security Advisory for golang : ALAS-2023-1760
<a href="#">355442</a> Amazon Linux Security Advisory for golang : ALAS2023-2023-209
<a href="#">355697</a> Amazon Linux Security Advisory for golang : ALAS2-2023-2163
<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="#">356428</a> Amazon Linux Security Advisory for amazon-ssm-agent : ALAS2-2023-2303
<a href="#">356458</a> Amazon Linux Security Advisory for amazon-ssm-agent : ALAS-2023-1866
<a href="#">356503</a> Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001
<a href="#">356574</a> Amazon Linux Security Advisory for docker : ALAS2ECS-2023-019
<a href="#">356580</a> Amazon Linux Security Advisory for docker : ALAS2DOCKER-2023-031
<a href="#">356591</a> Amazon Linux Security Advisory for docker : ALAS2NITRO-ENCLAVES-2023-030
<a href="#">378593</a> Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2023:0049)
<a href="#">378883</a> Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
<a href="#">379641</a> Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)
<a href="#">502993</a> Alpine Linux Security Update for go
<a href="#">503189</a> Alpine Linux Security Update for go
<a href="#">506082</a> Alpine Linux Security Update for go
<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="#">673313</a> EulerOS Security Update for golang (EulerOS-SA-2023-2613)
<a href="#">673314</a> EulerOS Security Update for golang (EulerOS-SA-2023-2583)
<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="#">691224</a> Free Berkeley Software Distribution (FreeBSD) Security Update for go (78f2e491-312d-11ee-85f2-bd89b893fcb4)
<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="#">770189</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3366)
<a href="#">770191</a> Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3409)
<a href="#">770193</a> Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:3545)
<a href="#">770195</a> Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:3612)
<a href="#">770203</a> Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2023:3910)
<a href="#">770204</a> Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:3914)

907917 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (26626-1)
908076 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (37428-1)
941126 AlmaLinux Security Update for go-toolset and golang (ALSA-2023:3318)
941127 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2023:3319)
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)
960938 Rocky Linux Security Update for go-toolset:Rocky (RLSA-2023:3319)

© [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](#)