



CVE-2023-29400

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-29400
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-11 16:15:00 UTC
Updated	2023-11-07 04:11:00 UTC
Description	Templates containing actions in unquoted HTML attributes (e.g. "attr={{.}}") executed with empty input can result in output v

Risk And Classification

Problem Types: CWE-74

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-2023-1753 - Go Packages	MISC	pkg.go.dev	
go.dev/cl/491617	MISC	go.dev	
html/template: improper handling of empty HTML attributes · Issue #59722 · golang/go · GitHub	MISC	go.dev	
[security] Go 1.20.4 and Go 1.19.9 are released	MISC	groups.google.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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 container-selinux (ELSA-2023-6474)

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)
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)
241856 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)
241924 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4459)
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)
242415 Red Hat Update for container-tools:rhel8 (RHSA-2023:6939)
242458 Red Hat Update for container-tools:4.0 (RHSA-2023:6938)
296101 Oracle Solaris 11.4 Support Repository Update (SRU) 59.138.2 Missing (CPUJUL2023)
355425 Amazon Linux Security Advisory for golang : ALAS-2023-1760
355442 Amazon Linux Security Advisory for golang : ALAS2023-2023-209
355697 Amazon Linux Security Advisory for golang : ALAS2-2023-2163
355748 Amazon Linux Security Advisory for golang : ALAS2023-2023-269
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
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
379641 Alibaba Cloud Linux Security Update for container-tools:rhel8 (ALINUX3-SA-2024:0050)
502993 Alpine Linux Security Update for go
503189 Alpine Linux Security Update for go

506082 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)
673313 EulerOS Security Update for golang (EulerOS-SA-2023-2613)
673314 EulerOS Security Update for golang (EulerOS-SA-2023-2583)
673548 EulerOS Security Update for golang (EulerOS-SA-2023-2644)
673694 EulerOS Security Update for golang (EulerOS-SA-2023-2686)
691224 Free Berkeley Software Distribution (FreeBSD) Security Update for go (78f2e491-312d-11ee-85f2-bd89b893fcb4)
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)
770200 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4093)
770202 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:4459)
907886 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (26627-1)
907914 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (26615-2)
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](#)