



CVE-2023-29405

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-29405 |
| State | PUBLIC |
| Assigner | security@golang.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-06-08 21:15:00 UTC |
| Updated | 2023-11-25 11:15:00 UTC |
| Description | The go command may execute arbitrary code at build time when using cgo. This may occur when running "go get" on a ma |

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 38 | All | All | All |
| Application | Golang | Go | All | All | All | All |

References

| Reference | Source | Link | Ta |
|---|---------|---|----|
| Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security | | security.gentoo.org | |
| cmd/go: improper sanitization of LDFLAGS [CVE-2023-29405] · Issue #60306 · golang/go · GitHub | MISC | go.dev | |
| GO-2023-1842 - Go Packages | MISC | pkg.go.dev | |
| [SECURITY] Fedora 38 Update: golang-1.20.6-1.fc38 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| go.dev/cl/501224 | MISC | go.dev | |
| [SECURITY] Fedora 37 Update: golang-1.19.12-1.fc37 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| [security] Go 1.20.5 and Go 1.19.10 are released | MISC | groups.google.com | |
| CVE Program record | CVE.ORG | www.cve.org | ca |
| NVD vulnerability detail | NVD | nvd.nist.gov | ca |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160768 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2023-3922)

160775 Oracle Enterprise Linux Security Update for go-toolset and golang (ELSA-2023-3923)

241761 Red Hat Update for go-toolset and golang (RHSA-2023:3923)

241765 Red Hat Update for go-toolset:rhel8 (RHSA-2023:3922)

284327 Fedora Security Update for golang (FEDORA-2023-eb60fcd505)

284380 Fedora Security Update for golang (FEDORA-2023-1819dc9854)

355697 Amazon Linux Security Advisory for golang : ALAS2-2023-2163

355748 Amazon Linux Security Advisory for golang : ALAS2023-2023-269

356180 Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-001

356503 Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001

378646 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2023:0055)

378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

503190 Alpine Linux Security Update for go

506083 Alpine Linux Security Update for go

673378 EulerOS Security Update for golang (EulerOS-SA-2023-2786)

673460 EulerOS Security Update for golang (EulerOS-SA-2023-2810)

673659 EulerOS Security Update for golang (EulerOS-SA-2023-2842)

673916 EulerOS Security Update for golang (EulerOS-SA-2023-2859)

710791 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)

754100 SUSE Enterprise Linux Security Update for go1.20 (SUSE-SU-2023:2526-1)

754101 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:2525-1)

907499 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (27110-1)

907867 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (27110-2)

907892 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (27123-1)

941157 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2023:3922)

941159 AlmaLinux Security Update for go-toolset and golang (ALSA-2023:3923)

960955 Rocky Linux Security Update for go-toolset and golang (RLSA-2023:3923)

© [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](#)