



CVE-2022-41716

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

Summary

CVE	CVE-2022-41716
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-02 16:15:00 UTC
Updated	2023-11-07 03:52:00 UTC
Description	Due to unsanitized NUL values, attackers may be able to maliciously set environment variables on Windows. In syscall.Star

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link	Tags
go.dev/cl/446916	MISC	go.dev	
[security] Go 1.19.3 and Go 1.18.8 are released	MISC	groups.google.com	
syscall, os/exec: unsanitized NUL in environment variables · Issue #56284 · golang/go · GitHub	MISC	go.dev	
GO-2022-1095 - Go Packages	MISC	pkg.go.dev	
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

[160322](#) Oracle Enterprise Linux Security Update for ol8addon (ELSA-2022-24267)

[160499](#) Oracle Enterprise Linux Security Update for ol8addon (ELSA-2023-18908)

183909 Debian Security Update for golang-1.19 (CVE-2022-41716)
354133 Amazon Linux Security Advisory for golang : ALAS2-2022-1887
354318 Amazon Linux Security Advisory for golist : ALAS2022-2022-240
354512 Amazon Linux Security Advisory for golang : ALAS2022-2022-239
354547 Amazon Linux Security Advisory for golang : ALAS-2022-239
354562 Amazon Linux Security Advisory for golist : ALAS-2022-240
354647 Amazon Linux Security Advisory for golist : ALAS2-2023-1913
355111 Amazon Linux Security Advisory for golist : ALAS2023-2023-046
355212 Amazon Linux Security Advisory for golang : ALAS2023-2023-048
378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
672476 EulerOS Security Update for golang (EulerOS-SA-2023-1035)
672519 EulerOS Security Update for golang (EulerOS-SA-2023-1010)
672528 EulerOS Security Update for golang (EulerOS-SA-2023-1100)
672533 EulerOS Security Update for golang (EulerOS-SA-2023-1124)
672621 EulerOS Security Update for golang (EulerOS-SA-2023-1385)
672650 EulerOS Security Update for golang (EulerOS-SA-2023-1357)
672761 EulerOS Security Update for golang (EulerOS-SA-2023-1505)
690973 Free Berkeley Software Distribution (FreeBSD) Security Update for go (26b1100a-5a27-11ed-abfe-29ac76ec31b5)
752815 SUSE Enterprise Linux Security Update for go1.18 (SUSE-SU-2022:4055-1)
752914 SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2022:4054-1)
754047 SUSE Enterprise Linux Security Update for go1.18-openssl (SUSE-SU-2023:2312-1)

© [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](#)