



# CVE-2022-24921

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

## Summary

<b>CVE</b>	CVE-2022-24921
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-05 20:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion via a deeply nested expression.

## Risk And Classification

**Problem Types:** CWE-674

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Astra Trident</a>	-	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 3395-1] golang-1.11 security update	MLIST	<a href="#">lists.debian.org</a>	
[security] Go 1.17.8 and Go 1.16.15 are released	CONFIRM	<a href="#">groups.google.com</a>	
CVE-2022-24921 Golang Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
<a href="#">cert-portal.siemens.com/productcert/pdf/ssa-744259.pdf</a>	MISC	<a href="#">cert-portal.siemens.com</a>	
[SECURITY] [DLA 2985-1] golang-1.7 security update	MLIST	<a href="#">lists.debian.org</a>	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	
[SECURITY] [DLA 2986-1] golang-1.8 security update	MLIST	<a href="#">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159783](#) Oracle Enterprise Linux Security Update for olcne istio istio (ELSA-2022-9362)

[159784](#) Oracle Enterprise Linux Security Update for olcne istio istio (ELSA-2022-9363)

[159885](#) Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14844)

[159886](#) Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14857)

[179209](#) Debian Security Update for golang-1.15 (CVE-2022-24921)

[179251](#) Debian Security Update for golang-1.7 (DLA 2985-1)

[179252](#) Debian Security Update for golang-1.8 (DLA 2986-1)

[181743](#) Debian Security Update for golang-1.11 (DLA 3395-1)

[240578](#) Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:5729)

[240607](#) Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2022:5068)

[353977](#) Amazon Linux Security Advisory for golang : ALAS2-2022-1811

[354041](#) Amazon Linux Security Advisory for golang : ALAS2-2022-1830

[378599](#) Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

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

[501856](#) Alpine Linux Security Update for go

[502093](#) Alpine Linux Security Update for go

[502299](#) Alpine Linux Security Update for go

[671610](#) EulerOS Security Update for golang (EulerOS-SA-2022-1534)

[671616](#) EulerOS Security Update for golang (EulerOS-SA-2022-1566)

[671754](#) EulerOS Security Update for golang (EulerOS-SA-2022-1805)

[671755](#) EulerOS Security Update for golang (EulerOS-SA-2022-1788)

[671783](#) EulerOS Security Update for golang (EulerOS-SA-2022-1841)

[671789](#) EulerOS Security Update for golang (EulerOS-SA-2022-1865)

[690818](#) Free Berkeley Software Distribution (FreeBSD) Security Update for go (e2af876f-a7c8-11ec-9a2a-002324b2fba8)

[710584](#) Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)

[752030](#) SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:1167-1)

[752032](#) SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2022:1164-1)

<a href="#">770160</a> Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5729)
<a href="#">770161</a> Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)
<a href="#">900730</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8876)
<a href="#">901879</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8898-1)
<a href="#">907784</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8876-1)
<a href="#">907845</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8898-2)
<a href="#">960300</a> Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2022:5337)
<a href="#">960612</a> Rocky Linux Security Update for go-toolset and golang (RLSA-2022:5799)

© [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](#)