



# CVE-2022-23772

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

## Summary

<b>CVE</b>	CVE-2022-23772
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-11 01:15:00 UTC
<b>Updated</b>	2022-11-09 21:51:00 UTC
<b>Description</b>	Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Mem

## Risk And Classification

### Problem Types: CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Golang	Go	All	All	All	All
Application	Netapp	Beegfs Csi Driver	-	All	All	All
Application	Netapp	Cloud Insights Telegraf Agent	-	All	All	All
Application	Netapp	Kubernetes Monitoring Operator	-	All	All	All
Application	Netapp	Storagegrid	-	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 2985-1] golang-1.7 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
February 2022 Golang Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[security] Go 1.17.7 and Go 1.16.14 are released	MISC	<a href="https://groups.google.com">groups.google.com</a>	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
[SECURITY] [DLA 2986-1] golang-1.8 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
Oracle Critical Patch Update Advisory - July 2022	N/A	<a href="https://www.oracle.com">www.oracle.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, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159810</a> Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2022-1819)
<a href="#">159886</a> Oracle Enterprise Linux Security Update for go-toolset:ol8addon (ELSA-2022-14857)
<a href="#">179228</a> Debian Security Update for golang-1.15 (CVE-2022-23772)
<a href="#">179251</a> Debian Security Update for golang-1.7 (DLA 2985-1)
<a href="#">179252</a> Debian Security Update for golang-1.8 (DLA 2986-1)
<a href="#">240276</a> Red Hat Update for go-toolset:rhel8 (RHSA-2022:1819)
<a href="#">240607</a> Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2022:5068)
<a href="#">241776</a> Red Hat Update for red hat openshift enterprise (RHSA-2023:3914)
<a href="#">353977</a> Amazon Linux Security Advisory for golang : ALAS2-2022-1811
<a href="#">354041</a> Amazon Linux Security Advisory for golang : ALAS2-2022-1830
<a href="#">354745</a> Amazon Linux Security Advisory for golang : ALAS-2023-1685
<a href="#">355216</a> Amazon Linux Security Advisory for golang : ALAS2023-2023-175
<a href="#">356304</a> Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-002
<a href="#">376494</a> Go Language Multiple Vulnerabilities
<a href="#">378599</a> Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)
<a href="#">378883</a> Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
<a href="#">501856</a> Alpine Linux Security Update for go
<a href="#">502093</a> Alpine Linux Security Update for go
<a href="#">502298</a> Alpine Linux Security Update for go
<a href="#">671610</a> EulerOS Security Update for golang (EulerOS-SA-2022-1534)
<a href="#">671754</a> EulerOS Security Update for golang (EulerOS-SA-2022-1805)
<a href="#">671755</a> EulerOS Security Update for golang (EulerOS-SA-2022-1788)
<a href="#">671783</a> EulerOS Security Update for golang (EulerOS-SA-2022-1841)
<a href="#">671789</a> EulerOS Security Update for golang (EulerOS-SA-2022-1865)
<a href="#">690794</a> Free Berkeley Software Distribution (FreeBSD) Security Update for go (096ab080-907c-11ec-bb14-002324b2fba8)

<a href="#">710584</a> Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
<a href="#">751793</a> SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2022:0724-1)
<a href="#">751800</a> SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:0723-1)
<a href="#">751818</a> OpenSUSE Security Update for go1.16 (openSUSE-SU-2022:0724-1)
<a href="#">751819</a> OpenSUSE Security Update for go1.17 (openSUSE-SU-2022:0723-1)
<a href="#">770161</a> Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)
<a href="#">770204</a> Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:3914)
<a href="#">900687</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8510)
<a href="#">901263</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8512-1)
<a href="#">907780</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8510-1)
<a href="#">907800</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8512-2)
<a href="#">940527</a> AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2022:1819)
<a href="#">960394</a> Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2022:1819)

© [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](#)**