



CVE-2022-23806

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

Summary

CVE	CVE-2022-23806
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-11 01:15:00 UTC
Updated	2023-04-20 00:15:00 UTC
Description	Curve.IsOnCurve in crypto/elliptic in Go before 1.16.14 and 1.17.x before 1.17.7 can incorrectly return true in situations with

Risk And Classification

Problem Types: CWE-252

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 3395-1] golang-1.11 security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2985-1] golang-1.7 security update	MLIST	lists.debian.org	
February 2022 Golang Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[security] Go 1.17.7 and Go 1.16.14 are released	MISC	groups.google.com	
Go: Multiple Vulnerabilities (GLSA 202208-02) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] [DLA 2986-1] golang-1.8 security update	MLIST	lists.debian.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159810](#) Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2022-1819)

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

[179225](#) Debian Security Update for golang-1.15 (CVE-2022-23806)

[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)

[240276](#) Red Hat Update for go-toolset:rhel8 (RHSA-2022:1819)

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

[240616](#) Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)

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

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

[354745](#) Amazon Linux Security Advisory for golang : ALAS-2023-1685

[355216](#) Amazon Linux Security Advisory for golang : ALAS2023-2023-175

[356304](#) Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-002

[376494](#) Go Language Multiple Vulnerabilities

[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

[502298](#) 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)

[671760](#) EulerOS Security Update for golang (EulerOS-SA-2022-1811)

671783 EulerOS Security Update for golang (EulerOS-SA-2022-1841)
671789 EulerOS Security Update for golang (EulerOS-SA-2022-1865)
690794 Free Berkeley Software Distribution (FreeBSD) Security Update for go (096ab080-907c-11ec-bb14-002324b2fba8)
710584 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202208-02)
751793 SUSE Enterprise Linux Security Update for go1.16 (SUSE-SU-2022:0724-1)
751800 SUSE Enterprise Linux Security Update for go1.17 (SUSE-SU-2022:0723-1)
751818 OpenSUSE Security Update for go1.16 (openSUSE-SU-2022:0724-1)
751819 OpenSUSE Security Update for go1.17 (openSUSE-SU-2022:0723-1)
770161 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:5068)
770162 Red Hat OpenShift Container Platform 4.10 Security Update (RHSA-2022:6094)
900668 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8521)
900988 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (8524-1)
904828 Common Base Linux Mariner (CBL-Mariner) Security Update for gcc (12331)
905143 Common Base Linux Mariner (CBL-Mariner) Security Update for gcc (12485)
905159 Common Base Linux Mariner (CBL-Mariner) Security Update for msft-golang (12568)
940527 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2022:1819)
960394 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](#)