



# CVE-2023-24532

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-24532
<b>State</b>	PUBLIC
<b>Assigner</b>	security@golang.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-08 20:15:00 UTC
<b>Updated</b>	2023-11-07 04:08:00 UTC
<b>Description</b>	The ScalarMult and ScalarBaseMult methods of the P256 Curve may return an incorrect result if called with some specific u

## Risk And Classification

**Problem Types:** CWE-682

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All

## References

Reference	Source
crypto/elliptic: specific unreduced P-256 scalars produce incorrect results (CVE-2023-24532) · Issue #58647 · golang/go · GitHub	MISC
GO-2023-1621 - Go Packages	MISC
go.dev/cl/471255	MISC
[security] Go 1.20.2 and Go 1.19.7 are released	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 184193 Debian Security Update for golang-1.19 (CVE-2023-24532)
- 296100 Oracle Solaris 11.4 Support Repository Update (SRU) 58.144.3 Missing (CPUAPR2023)

<a href="#">354890</a> Amazon Linux Security Advisory for golang : ALAS2-2023-2015
<a href="#">354901</a> Amazon Linux Security Advisory for golang : ALAS-2023-1731
<a href="#">355216</a> Amazon Linux Security Advisory for golang : ALAS2023-2023-175
<a href="#">355697</a> Amazon Linux Security Advisory for golang : ALAS2-2023-2163
<a href="#">355797</a> Amazon Linux Security Advisory for containerd : ALAS2NITRO-ENCLAVES-2023-026
<a href="#">355837</a> Amazon Linux Security Advisory for containerd : ALAS2DOCKER-2023-029
<a href="#">356180</a> Amazon Linux Security Advisory for golang : ALASGOLANG1.19-2023-001
<a href="#">356503</a> Amazon Linux Security Advisory for golang : ALAS2GOLANG1.19-2023-001
<a href="#">502862</a> Alpine Linux Security Update for go
<a href="#">503187</a> Alpine Linux Security Update for go
<a href="#">506080</a> Alpine Linux Security Update for go
<a href="#">691086</a> Free Berkeley Software Distribution (FreeBSD) Security Update for go (742279d6-bdbe-11ed-a179-2b68e9d12706)
<a href="#">753772</a> SUSE Enterprise Linux Security Update for go1.19 (SUSE-SU-2023:0733-1)
<a href="#">753839</a> SUSE Enterprise Linux Security Update for container-suseconnect (SUSE-SU-2023:0871-1)
<a href="#">908039</a> Common Base Linux Mariner (CBL-Mariner) Security Update for golang (37385-1)

© [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](#)**