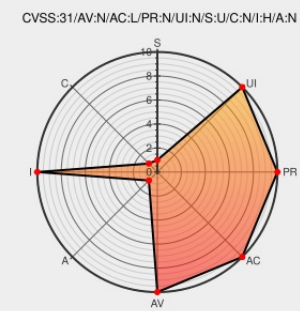
CVE-2023-24533

Published on: Not Yet Published

Last Modified on: 03/15/2023 05:58:00 PM UTC

CVE-2023-24533

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nistec from Nistec Project contain the following vulnerability:

Multiplication of certain unreduced P-256 scalars produce incorrect results. There are no protocols known at this time that can be attacked due to this.

CVE-2023-24533 has been assigned by security@golang.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **filippo.io/nistec** - **filippo.io/nistec** version **< 0.0.2**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVE References

Description	Tags	Link
crypto/internal/nistec: reduce P-256 scalar · FiloSottile/nistec@c58aa12 · GitHub	github.com text/html	MISC github.com/FiloSottile/nistec/commit/c58aa1223ccf3943513e1e661cebce95af137244
crypto/elliptic: specific unreduced P-256 scalars produce incorrect results (CVE-2023-24532) · Issue #58647 · golang/go · GitHub	go.dev text/html	MISC go.dev/issue/58647
GO-2023-1595 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2023-1595

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nistec Project	Nistec	All	All	All	All

cpe:2.3:a:nistec_project:nistec:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2023-24533	2023-03-08 21:38:09

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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