CVE-2022-39213

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-39213
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-15 22:15:00 UTC
Updated	2023-08-18 15:22:00 UTC
Description	go-cvss is a Go module to manipulate Common Vulnerability Scoring System (CVSS). In affected versions when a full CVS

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Go-cvss Project	Go-cvss	All	All	All	All
Application	Pandatix	Go-cvss	All	All	All	All

References

Reference	Source	Link
Improve CVSS v2.0 implementation (0/1 allocs/op) · pandatix/go-cvss@d9d478f · GitHub	MISC	github.com
go-cvss/SECURITY.md at master · pandatix/go-cvss · GitHub	MISC	github.com
Out-of-bounds Read in github.com/pandatix/go-cvss/20 ParseVector function · Advisory · pandatix/go-cvss · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report