CVE-2023-27560

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

Summary

CVE	CVE-2023-27560
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-03 06:15:00 UTC
Updated	2023-03-10 18:54:00 UTC
Description	Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields.

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpseclib	Phpseclib	All	All	All	All

References

Reference	Source	Link	Tags
PrimeField: prevent infinite loop with composite primefields · phpseclib/phpseclib@6298d1c · GitHub	MISC	github.com	
Release 3.0.19 · phpseclib/phpseclib · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182710 Debian Security Update for php-phpseclib3 (CVE-2023-27560)

6000504 Debian Security Update for phpseclib (DLA 3749-1)

6000505 Debian Security Update for php-phpseclib (DLA 3750-1)

Free CVE JSON API cve.report/api

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