CVE-2021-30130

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

Summary

CVE	CVE-2021-30130
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-06 15:15:00 UTC
Updated	2023-01-27 19:52:00 UTC
Description	phpseclib before 2.0.31 and 3.x before 3.0.7 mishandles RSA PKCS#1 v1.5 signature verification.

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Phpseclib	Phpseclib	All	All	All	All

References

Reference	Sour
[SECURITY] [DLA 3198-1] php-phpseclib security update	MLIS
Release 2.0.31 · phpseclib/phpseclib · GitHub	CON
[SECURITY] [DLA 3197-1] phpseclib security update	MLIS
Release 3.0.7 · phpseclib/phpseclib · GitHub	CON
cleanup RSA PKCS#1 v1.5 signature verification (CVE-2021-30130) by terrafrost · Pull Request #1635 · phpseclib/phpseclib · GitHub	MISC
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179459 Debian Security Update for phpseclibphp-phpseclib (CVE-2021-30130)

181232 Debian Security Update for php-phpseclib (DLA 3198-1)

181233 Debian Security Update for phpseclib (DLA 3197-1)

Free CVE JSON API cve.report/api

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