phpseclib's AES-CBC unpadding susceptible to padding oracle timing attack

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

Summary

CVE	CVE-2026-32935
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-20 03:16:00 UTC
Updated	2026-05-08 16:16:10 UTC
Description	phpseclib is a PHP secure communications library. Projects using versions 0.1.1 through 1.0.26, 2.0.0 through 2.0.51, and

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-208 | CWE-208 CWE-208: Observable Timing Discrepancy

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/
4.0	CNA	DECLARED	8.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Phpseclib	Phpseclib	affected >= 3.0.0, < 3.0.50	Not specified
CNA	Phpseclib	Phpseclib	affected >= 2.0.0, < 2.0.52	Not specified

CNA	Phpseclib	Phpseclib	affected >= 0.1.1, < 1.0.27	Not specified

References

Reference	Source	Link	Tags
github.com/phpseclib/phpseclib/commit/ccc21aef71eb170e9bf819b167e67d1fd9...	security-advisories@github.com	github.com	Patch
github.com/phpseclib/phpseclib/security/advisories/GHSA-94g3-g5v7-q4jg	security-advisories@github.com	github.com	Patch,
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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