CVE-2019-9082

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

Summary

CVE	CVE-2019-9082
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-24 18:29:00 UTC
Updated	2022-04-05 20:42:00 UTC
Description	ThinkPHP before 3.2.4, as used in Open Source BMS v1.1.1 and other products, allows Remote Command Execution via p

Risk And Classification

EPSS: 0.942550000 probability, percentile 0.999340000 (date 2026-04-22)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-94 | CWE-306

CISA Known Exploited Vulnerability

Vendor	ThinkPHP
Product	ThinkPHP
Name	ThinkPHP Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-9082

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensourcebms	Open Source Background Management System	1.1.1	All	All	All
Application	Opensourcebms	Open Source Background Management System	1.1.1	All	All	All
Application	Thinkphp	Thinkphp	All	All	All	All
Application	Thinkphp	Thinkphp	All	All	All	All
Application	Zzzcms	Zzzphp	1.6.1	All	All	All
Application	Zzzcms	Zzzphp	1.6.1	All	All	All

References

Reference	Source	Link	T
zzzphp CMS 1.6.1 - Cross-Site Request Forgery - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	E
ThinkPHP 5.0.23 Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
There is A RCE vulnerability in your system. · Issue #33 · xiayulei/open_source_bms · GitHub	MISC	github.com	E
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	ke

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

13517 ThinkPHP Remote Code Execution (RCE) Vulnerability