



# CVE-2019-9082

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-9082
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-24 18:29:00 UTC
<b>Updated</b>	2022-04-05 20:42:00 UTC
<b>Description</b>	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

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Opensourcebms</a>	<a href="#">Open Source Background Management System</a>	1.1.1	All	All	All
Application	<a href="#">Opensourcebms</a>	<a href="#">Open Source Background Management System</a>	1.1.1	All	All	All
Application	<a href="#">Thinkphp</a>	<a href="#">Thinkphp</a>	All	All	All	All
Application	<a href="#">Thinkphp</a>	<a href="#">Thinkphp</a>	All	All	All	All
Application	<a href="#">Zzzcms</a>	<a href="#">Zzzphp</a>	1.6.1	All	All	All
Application	<a href="#">Zzzcms</a>	<a href="#">Zzzphp</a>	1.6.1	All	All	All

## References

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

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

13517 ThinkPHP Remote Code Execution (RCE) Vulnerability

© [CVE.report](http://CVE.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

Free CVE JSON API [cve.report/api](http://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)