Surge in attacks exploiting old ThinkPHP and ownCloud flaws

By
Bill Toulas

- February 12, 2025
- 06:04 PM
- 0

Increased hacker activity has been observed in attempts to compromise poorly maintained devices that are vulnerable to older security issues from 2022 and 2023.

Threat monitoring platform GreyNoise is reporting spikes in actors leveraging CVE-2022-47945 and CVE-2023-49103 that affect ThinkPHP Framework and the open-source ownCloud solution for file sharing and syncing.

Both vulnerabilities have critical severity and can be exploited to execute arbitrary operating system commands or to obtain sensitive data (e.g. admin password, mail server credentials, license key).

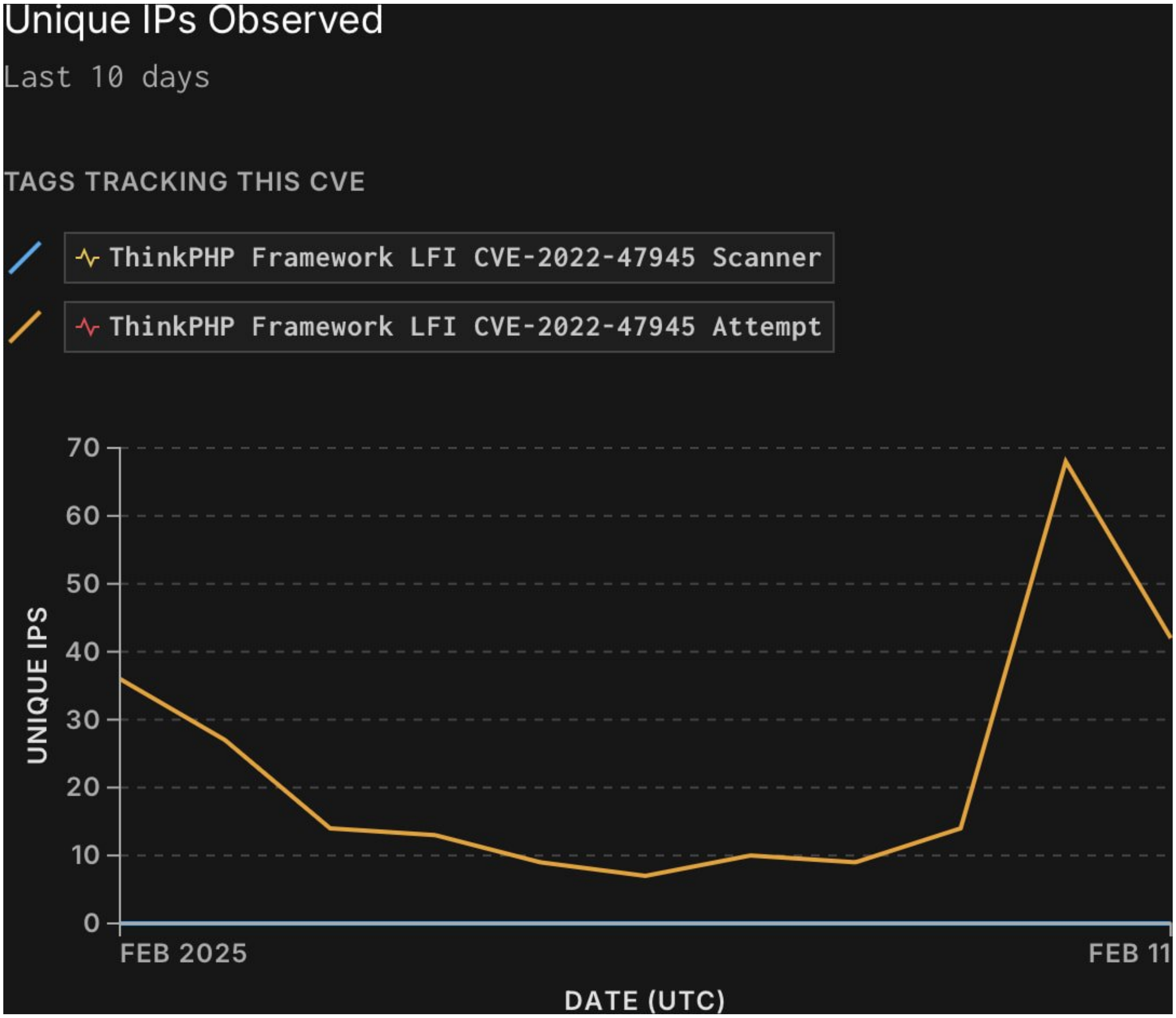
The first vulnerability is a local file inclusion (LFI) issue in the language parameter of ThinkPHP Framework before 6.0.14. An unauthenticated remote attacker can leverage it to execute arbitrary operating system commands in deployments where the language pack feature is enabled.

Akamai reported last summer that Chinese threat actors have been leveraging the flaw since October 2023 in narrow-scope operations.

According to threat monitoring platform GreyNoise, CVE-2022-47945 is under high-volume exploitation right now, with attacks launched from a growing number of source IPs.

"GreyNoise has observed 572 unique IPs attempting to exploit this vulnerability, with activity increasing in recent days," warns the bulletin.

This is despite its low Exploit Prediction Scoring System (EPSS) rating of 7% and the flaw not being included in CISA's Known Exploited Vulnerabilities (KEV) catalog.



Daily exploitation activity
Source: Greynoise

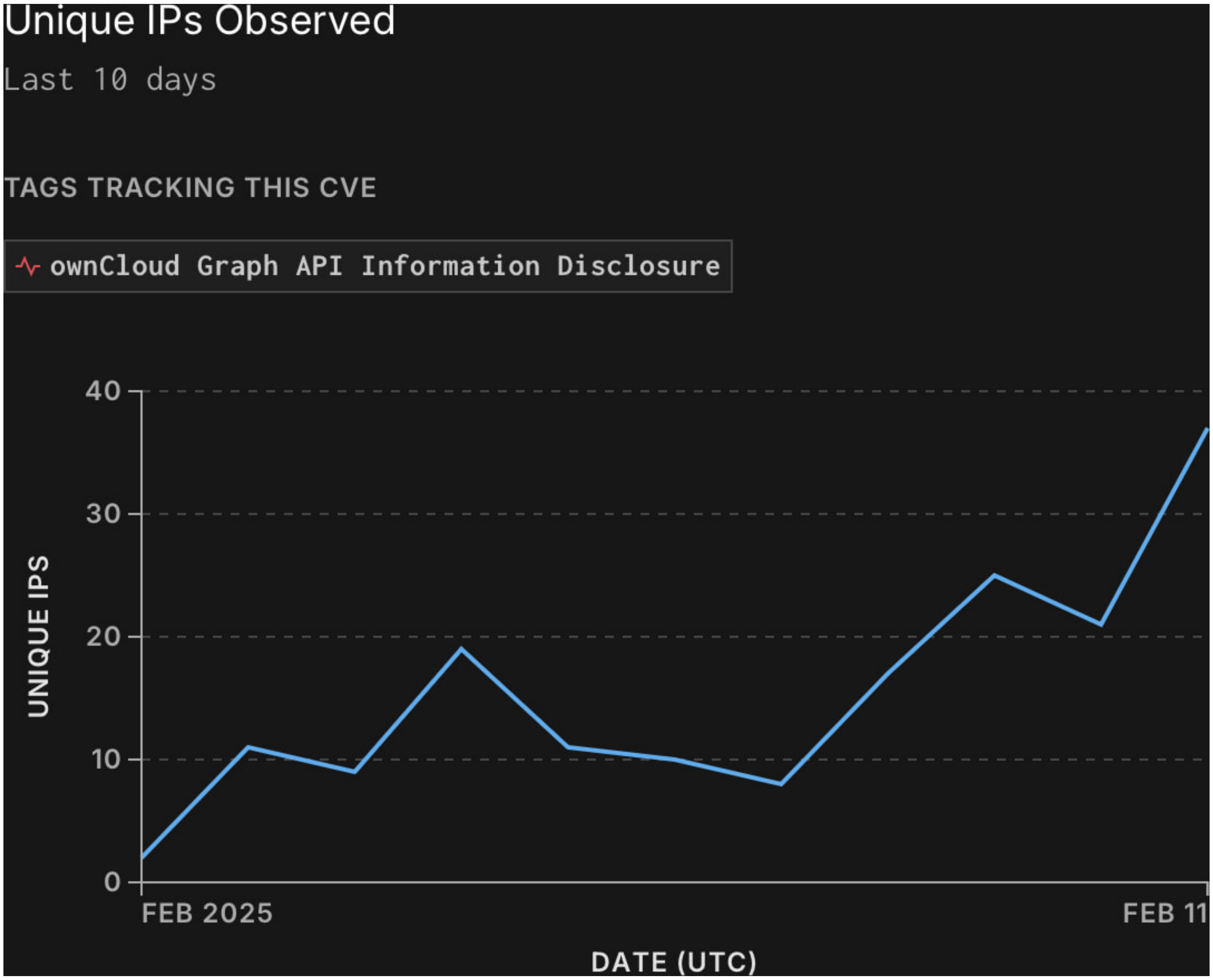
The second vulnerability affects the popular open-source file-sharing software and arises from the app's dependency on a third-party library that exposes PHP environment details through a URL.

Soon after the vulnerability's initial disclosure from the developers in November 2023, hackers started exploiting it to steal sensitive information from unpatched systems.

A year later, CVE-2023-49103 was listed by the FBI, CISA, and NSA, among the 15 most exploited vulnerabilities of 2023.

Despite over 2 years having passed since the vendor released an update that addresses the security issue, many instances remain unpatched and exposed to attacks.

GreyNoise observed increased exploitation of CVE-2023-49103 recently, with malicious activity originating from 484 unique IPs.



IPs targeting ownCloud daily
Source: Greynoise

To safeguard systems against active exploitation users are advised to upgrade to ThinkPHP 6.0.14 or later, and ownCloud GraphAPI to 0.3.1 and newer.

It is also recommended that potentially vulnerable instances are taken offline or placed behind a firewall to reduce the attack surface.

RED REPORT™
BY PICUS SECURITY
2025
PICUS
RED REPORT
2025
The Top 10 Most Prevalent MITRE ATT&CK® Techniques
SneakThief and The Perfect Heist
Top 10 MITRE

Related Articles:

CentreStack RCE exploited as zero-day to breach file sharing servers

New Mirai botnet behind surge in TVT DVR exploitation

Newest Ivanti SSRF zero-day now under mass exploitation

Ivanti Connect Secure zero-days exploited to deploy custom malware

Critical auth bypass bug in CrushFTP now exploited in attacks

- Actively Exploited
- OwnCloud
- ThinkPHP
- Vulnerability

Bill Toulas

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: