Rising Attacks Targeting Vulnerabilities in ThinkPHP and ownCloud

Description


ESL-NEWS.COM

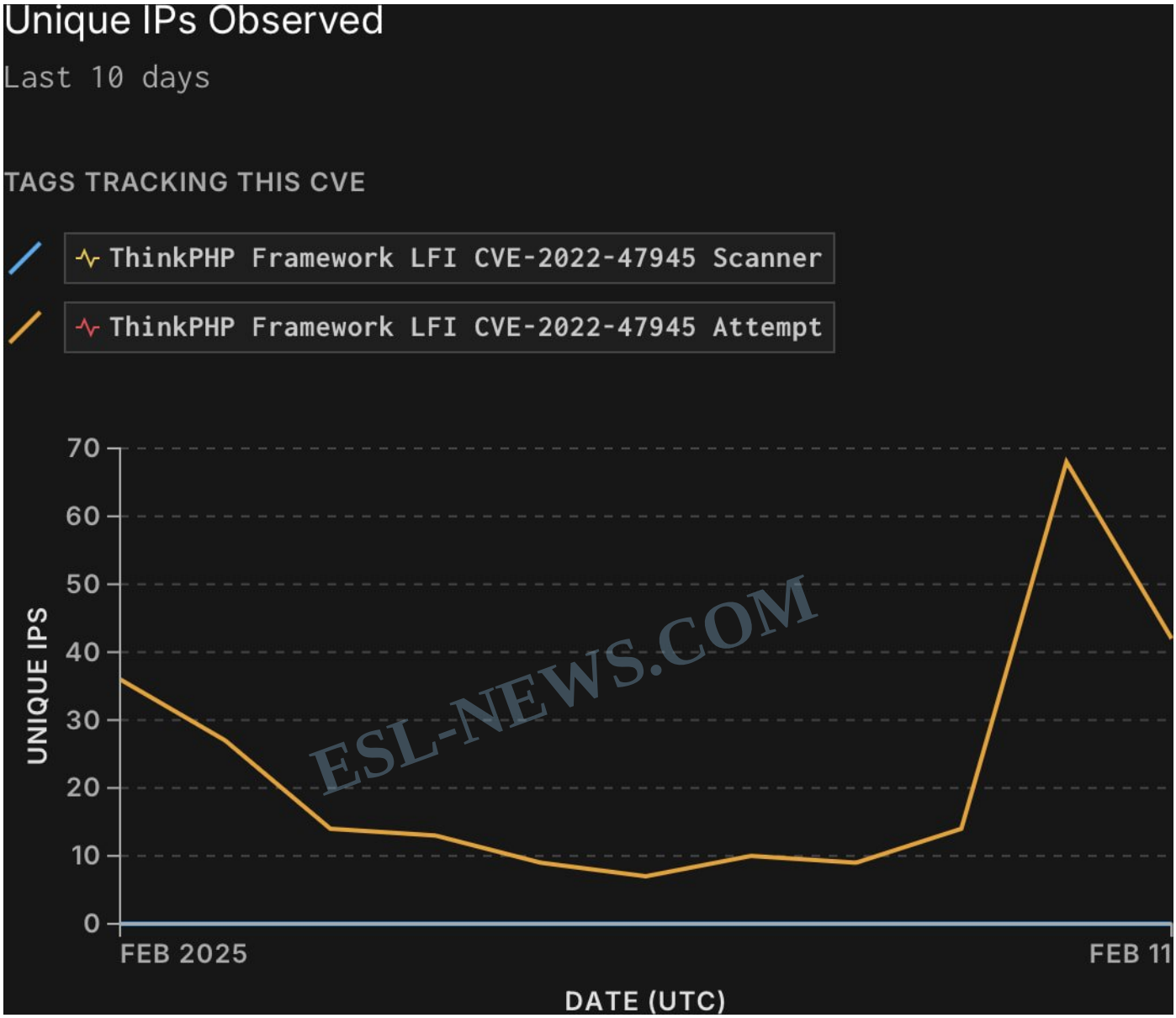
Recent months have witnessed a surge in hacker activity targeting inadequately maintained devices vulnerable to older security flaws from 2022 and 2023.

According to the threat monitoring platform GreyNoise, there has been a marked increase in attempts by cybercriminals to exploit CVE-2022-47945 and CVE-2023-49103, which affect the ThinkPHP Framework and the open-source file-sharing solution ownCloud.

Both vulnerabilities carry critical severity ratings and can be exploited to execute arbitrary operating system commands or to extract sensitive data, such as administrator credentials and mail server information.

The first, CVE-2022-47945, involves a local file inclusion (LFI) problem in the ThinkPHP Framework, impacting versions prior to 6.0.14. An attacker can remotely exploit this vulnerability in environments where the language pack feature is enabled.

Akamai reported that Chinese threat actors have been actively exploiting this flaw since October 2023 for limited-scope operations. Recently, GreyNoise noted that 572 unique IP addresses have attempted to exploit CVE-2022-47945, with activity on the rise.

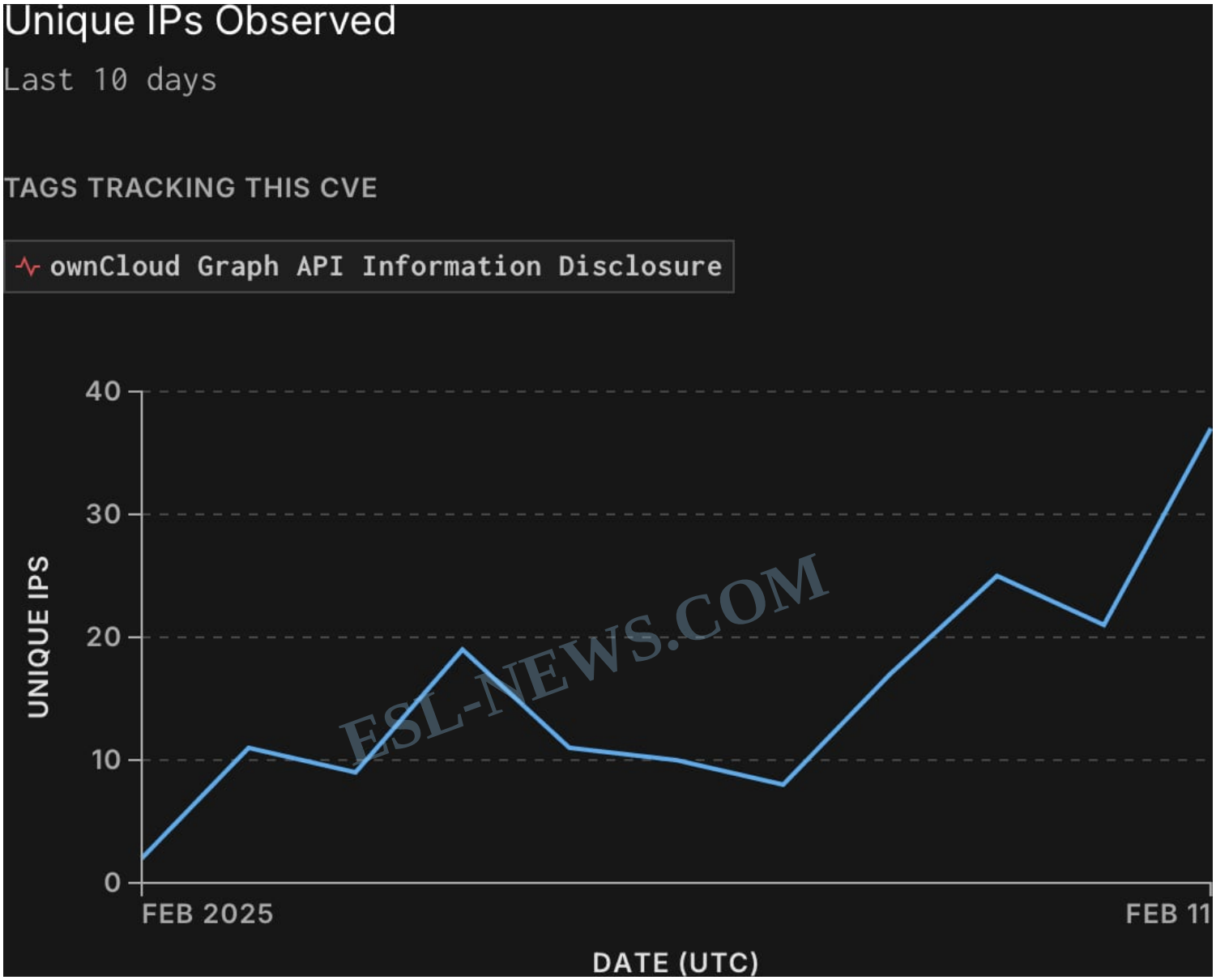


Daily exploitation activity

Source: GreyNoise

The second vulnerability, CVE-2023-49103, affects the widely used ownCloud software due to its reliance on a vulnerable third-party library. After its disclosure in November 2023, hackers quickly began exploiting this flaw to obtain sensitive information from unpatched systems.

Despite over two years since the vendor's last security update, many instances of ownCloud remain unpatched and vulnerable. GreyNoise has recently noted an uptick in attacks originating from 484 unique IPs targeting this flaw.



IPs targeting ownCloud daily

Source: GreyNoise

To mitigate these risks, users are strongly advised to upgrade to ThinkPHP version 6.0.14 or later, and ownCloud GraphAPI to version 0.3.1 or newer. Vulnerable systems should also be taken offline or secured behind a firewall to minimize exposure.

Vocabulary List:

1. **Vulnerability** /ˌvʌl.nəˈbɪl.ɪ.ti/ (noun): The quality of being open to damage or attack.
2. **Exploitation** /ˌɛk.splɔɪˈteɪ.ʃən/ (noun): The action of making full use of and benefiting from resources.
3. **Severity** /səˈver.ɪ.ti/ (noun): The condition of being very bad or serious.

4. **Mitigate** /ˈmɪt.ɪ.geɪt/ (verb): To make less severe serious or painful.
5. **Extraction** /ɪkˈstræk.ʃən/ (noun): The action of taking out something especially using effort or force.
6. **Unpatched** /ʌnˈpætʃt/ (adjective): Referring to software or a system that has not been updated with security fixes.

Comprehension Questions

Multiple Choice

1. Which vulnerabilities have cybercriminals been attempting to exploit according to GreyNoise?

   Option: CVE-2021-5543 and CVE-2022-87329
   Option: CVE-2022-47945 and CVE-2023-49103
   Option: CVE-2024-12345 and CVE-2024-67890
   Option: CVE-2023-91023 and CVE-2022-76543

2. What problem is associated with CVE-2022-47945 in the ThinkPHP Framework?

   Option: Local file inclusion
   Option: SQL injection
   Option: Cross-site scripting
   Option: Directory traversal

3. How many unique IP addresses have attempted to exploit CVE-2022-47945?

   Option: 572
   Option: 315
   Option: 869
   Option: 721

4. Which widely used software is affected by CVE-2023-49103?

   Option: FileZilla
   Option: Dropbox
   Option: ownCloud
   Option: Evernote

5. What action are users advised to take to mitigate risks associated with these vulnerabilities?

   Option: Upgrade to ThinkPHP version 6.0.12
   Option: Keep systems offline permanently
   Option: Secure behind a firewall

Option: Disable all security features

6. What kind of operations were Chinese threat actors conducting with CVE-2022-47945 in October 2023?

Option: Large-scale attacks
Option: Limited-scope operations
Option: Cyber espionage
Option: Data breaches

True-False

7. CVE-2022-47945 impacts ownCloud software.

8. Vulnerable systems should be taken offline to minimize exposure.

9. GreyNoise recently noted an increase in the exploitation of CVE-2023-49103.

10. The local file inclusion problem in ThinkPHP affects versions 6.0.14 and later.

11. CVE-2023-49103 was disclosed in October 2023.

12. Akamai reported an increase in activity related to CVE-2022-47945.

Gap-Fill

13. Chinese threat actors have been actively exploiting CVE-2022-47945 since October 2023 for _____ operations.

14. It is strongly advised to upgrade to ThinkPHP version _____ to mitigate risks.

15. Many instances of ownCloud remain unpatched despite over two years since the vendor's last security update in _____.

16. Users should secure vulnerable systems behind a firewall to minimize _____.

17. The vulnerability CVE-2023-49103 affects ownCloud due to its reliance on a vulnerable third-party _____.

18. GreyNoise noted an uptick in attacks originating from 484 unique _____ targeting the flaw in ownCloud.

Answer

Multiple Choice: 1. CVE-2022-47945 and CVE-2023-49103 2. Local file inclusion 3. 572 4. ownCloud 5. Secure behind a firewall 6. Limited-scope operations
True-False: 7. False 8. True 9. True 10. False 11. False 12. True
Gap-Fill: 13. limited-scope 14. 6.0.14 15. 2012 16. exposure 17. library 18. IPs

Answer

CATEGORY

1. Sci/Tech - LEVEL4

Date Created
2025/02/13
Author
aimeeyoung99