F#RTINET.

OUTBREAK ALERTS





Apache HTTP Server Path Traversal Vulnerability

Apache webservers running an older and vulnerable version of Apache 2.4.49 and 2.4.50 are still deployed on various could platforms. According to

Attackers still targeting Apache Path Traversal vulnerability in high volumes https://httpd.apache.org/security/vulnerabilities_24.html

CVEs: CVE-2021-42013, CVE-2021-41773

Shodan, 6000+ webservers could still be vulnerable to a path traversal attack and can eventually lead to remote code execution.

Background Apache HTTP Server Project released a security advisory about a year ago on a path traversal and file disclosure

Announced

October 7, 2021: Apache released update 2.4.51 which fixes both CVE-2021-41773 and CVE-2021-42013.

vulnerability in Apache HTTP Server 2.4.49 and 2.4.50 tracked as CVE-2021-41773 and CVE-2021-42013.

Latest Developments

September 12, 2022: According to FortiGuard research, CVE-2021-42013 and CVE-2021-41773 are seen in high attack attempts worldwide with an average of 40,000 device detections. It is strongly advised to update vulnerable Apache servers as soon as possible if not already updated. June 8, 2022: Latest Apache HTTP Server version 2.4.54 released.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

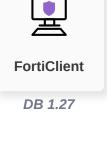
Reconnaissance

Delivery

Vulnerability

Weaponization

Detects systems vulnerable to the Apache Path Traversal Vulnerability, and auto-patches when possible. (CVE-2021-42013, CVE-2021-41773)



Exploitation

IPS

Block attack attempts related to Apache Path Traversal (CVE-2021-42013, CVE-2021-41773)

FortiGate

DB 18.173

Web App Security

FortiSASE

FortiADC

DB 0.00302

DB 18.173

FortiNDR DB 18.173

FortiADC DB 18.173

FortiProxy DB 18.173

Block attack attempts related to Apache Path Traversal (CVE-2021-42013, CVE-2021-41773)



Installation C2

Action

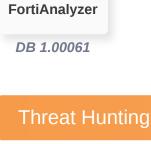


alert and generate reports:

DETECT

Outbreak Detection

Find and correlate important information to identify an outbreak, the following updates are available to raise









FortiSIEM

FortiSIEM

v6.4+





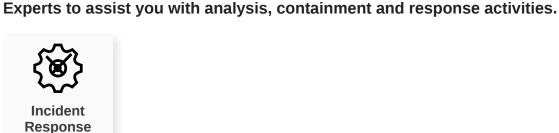
Services that can automatically respond to this outbreak.

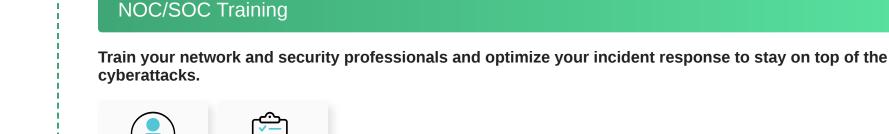
Assisted Response Services

Automated Response

FortiXDR

Develop containment techniques to mitigate impacts of security events:





cyberattacks.

and other forms of cyberattacks.

Response

Readiness

RECOVER

(and recovery from) security incidents:

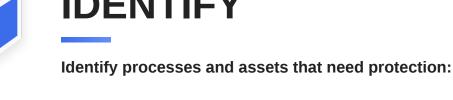
End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download

Improve security posture and processes by implementing security awareness and training, in preparation for



NSE Training



IDENTIFY

Attack Surface Hardening

Rating

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Additional Resources

Threat Signal

Apache Advisory https://httpd.apache.org/security/vulnerabilities 24.html https://www.fortiguard.com/threat-signal-report/4173

Learn more about FortiGuard Outbreak Alerts