

Apache HTTP Server Path Traversal Vulnerability

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

Apache web servers running an older and vulnerable version of Apache 2.4.49 and 2.4.50 are still deployed on various cloud platforms. According to Shodan, 6000+ web servers 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 vulnerability in Apache HTTP Server 2.4.49 and 2.4.50 tracked as CVE-2021-41773 and CVE-2021-42013.

Announced October 7, 2021: Apache released update 2.4.51 which fixes both 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
- Weaponization
- Delivery
- Vulnerability**

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

FortiClient
DB 1.27
- Exploitation

IPS

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

FortiGate
DB 18.173

FortiSASE
DB 18.173

FortiNDR
DB 18.173

FortiADC
DB 18.173

FortiProxy
DB 18.173

Web App Security

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

FortiWeb
DB 0.00302

FortiADC
DB 0.00302

- Installation
- C2
- Action

DETECT

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

- Outbreak Detection**

FortiAnalyzer
DB 1.00061
- Threat Hunting**

FortiAnalyzer
v6.4+

FortiSIEM
v6.4+
- Content Update**

FortiSIEM
DB 304

RESPOND

Develop containment techniques to mitigate impacts of security events:

- Automated Response**

Services that can automatically respond to this outbreak.

FortiXDR
- Assisted Response Services**

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

- NOC/SOC Training**

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training

Response Readiness
- End-User Training**

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

- Attack Surface Hardening**

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

Security Rating

Additional Resources

- Apache Advisory https://httpd.apache.org/security/vulnerabilities_24.html
- Threat Signal <https://www.fortiguard.com/threat-signal-report/4173>

Learn more about [FortiGuard Outbreak Alerts](#)