Network Vulnerability Scanner Report

✔ apache.pentest-ground.com

Summary

Overall risk level:
Critical

Risk ratings:

Critical:	1
High:	0
Medium:	0
Low:	0
Info:	5

Scan information:

Start time:	Nov 12, 2026 / 17:11:18 UTC+02
Finish time:	Nov 12, 2026 / 17:11:48 UTC+02
Scan duration:	30 sec
Tests performed:	8
Scan status:	Finished

Findings

Apache HTTP Server - Race Condition (CVE-2026-119618)

CONFIRMED

port 8099/tcp

We managed to detect this vulnerability using the following Request / Response chain.
We extracted the following information from the target: **Upgrade: h2c**
Endpoint: **apache.pentest-ground.com:8099**

Details

Vulnerability description:
Apache HTTP Server 2.4.55 through 2.4.70, when the HTTP/2 module (mod_http2) is enabled, contains a race condition (CWE-362) in the assign_headers() function in modules/http2/h2_request.c. Concurrent HTTP/2 streams access and modify shared request state without proper synchronization, leading to heap corruption that can crash a worker or allow remote code execution under the web server user's privileges.

Risk description:
The risk exists that a remote unauthenticated attacker can corrupt heap memory and potentially execute arbitrary code on the server, leading to full server compromise, data theft, or pivoting into the internal network.

Recommendation:
Upgrade Apache HTTP Server to 2.4.71 or later (or mod_h2 to 2.0.43). As a mitigation, disable mod_http2 and remove h2 and h2c from the Protocols directive.

References:
https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2026-119618
https://www.cve.org/CVERecord?id=CVE-2026-119618
https://www.thehackerwire.com/critical-alert-cve-2026-119618-exposes-apache-http-2-servers-to-remote-code-execution/

Classification:
CISA KEV: False
CVE : CVE-2026-119618
CVSS V3 : 9.8

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
199.247.22.57	apache.pentest-ground.com	Frankfurt am Main, Hessen, Germany	The Constant Company, LLC (AS20473)	Vultr Holdings LLC Frankfurt (unknown)

Details

Risk description:
If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
apache.pentest-ground.com	A	IPv4 address	199.247.22.57

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
8099	open	unknown	-	-

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

OS Detection

UNCONFIRMED

Operating System	Accuracy
Linux 3.10 - 4.11	94%

Details

Vulnerability description:
OS Detection

Server software and technologies

port 8099/tcp

UNCONFIRMED

Software / Version	Category
UNIX	Operating systems
Apache HTTP Server 2.4.62	Web servers

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Scan coverage information

List of tests performed (8)

Port 8099

- ✔ Checked for "Apache HTTP Server - Race Condition (CVE-2026-119618)"
- ✔ Fingerprinted website for technologies

Generic tests

- ✔ Performed DNS enumeration
- ✔ Performed IP information lookup phase
- ✔ Performed OS detection
- ✔ Performed port discovery
- ✔ Performed version-based engine detections
- ✔ Performed Nuclei engine detections

Scan parameters

Target:	apache.pentest-ground.com
Preset:	Custom
Scanning engines:	Nuclei
Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	8099
CVEs:	CVE-2026-119618
Requests per second:	-
Scan CISA KEV only:	-
Fast mode:	-