Network Vulnerability Scanner Report

✔ **php2shell.pentest-ground.com**

Summary

Overall risk level:

Critical

Risk ratings:

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

Scan information:

Start time:	Oct 22, 2026 / 17:16:06 UTC+03
Finish time:	Oct 22, 2026 / 17:16:46 UTC+03
Scan duration:	40 sec
Tests performed:	10
Scan status:	Finished

Findings

PHP2Shell - Remote Code Execution (CVE-2026-109618 & CVE-2026-109619)

CONFIRMED

port 443/tcp

We managed to detect this vulnerability using the following Request / Response chain.
Endpoint: **https://php2shell.pentest-ground.com:443/index.php**

Details

Vulnerability description:

PHP versions prior to 8.2.35, 8.3.36, 8.4.27 and 8.5.12 contain an uncontrolled memory consumption vulnerability caused by the parsing of a multipart/form-data request body that contains many part headers and deeply nested array field names. An unauthenticated attacker can send a crafted multipart request that exhausts the configured memory limit, aborting request processing and leading to denial of service. Official fixed releases exist only for the 8.2, 8.3, 8.4 and 8.5 branches. PHP 8.1, 8.0 and 7.4 are end-of-life and get no new releases, but the PHP security team published minimal source backports for them, and some Linux distributions and LTS vendors ship backported packages. PHP 7.3 and earlier have no official fix. Detection sends a small multipart request to /index.php as a baseline, then retries with bodies of roughly 1 MB, 8 MB and 20 MB, stopping at the first hit, and matches when PHP returns an "Allowed memory size exhausted" error or when the baseline served a page but the large request comes back empty or as a 502-504 gateway error.

Risk description:

A match means the server handled the oversized multipart body the way vulnerable PHP builds do. It does not prove that code execution is possible on this host. Keep in mind that the scan itself is not free: the 8 MB and 20 MB probes can use a lot of memory and may kill the PHP worker that receives them.

Recommendation:

Upgrade PHP to 8.2.35, 8.3.36, 8.4.27, 8.5.12 or later. These fix both CVE-2026-109618 and CVE-2026-109619. On PHP 8.1, 8.0 or 7.4, install a backported package from your distribution or LTS vendor, or build from the PHP security team's source backport branches (PHP-7.4/8.0/8.1-CVE-2026-109618-109619 in php-src). PHP 7.3 and older have no fix and must be upgraded to a supported release. While you're in php.ini, set expose_php = Off so the server stops advertising its PHP version in response headers.

References:

https://nvd.nist.gov/vuln/detail/CVE-2026-109618
https://www.php.net/ChangeLog-8.php
https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
https://github.com/php/php-src/tree/PHP-7.4-CVE-2026-109618-109619
https://github.com/php/php-src/tree/PHP-8.0-CVE-2026-109618-109619
https://github.com/php/php-src/tree/PHP-8.1-CVE-2026-109618-109619

Classification:

CISA KEV: False
CVE : CVE-2026-109618
CVSS V3 : 9.2

Vulnerabilities found for PHP 8.2.34

UNCONFIRMED

port 443/tcp

CVE	CVSS	EPSS Score	EPSS Percentile	CISA KEV	Summary	Exploit

CVE-2026-109619	9.2	N/A	N/A	No	PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).	N/A
CVE-2026-109618	9.2	N/A	N/A	No	PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).	N/A

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one) for any of these vulnerabilities and use it to attack the system.

Notes:
- The vulnerabilities are identified based on the server's version.
- Only the first 5 vulnerabilities with the highest risk are shown for each port.

Since the vulnerabilities were discovered using only version-based testing, the risk level for this finding will not exceed "high" severity. Critical risks will be assigned to vulnerabilities identified through accurate active testing methods.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risks imposed by these vulnerabilities.

Classification:
CISA KEV: False
CVE : CVE-2026-109619, CVE-2026-109618
CVSS V3 : 9.2

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
45.77.55.213	php2shell.pentest-ground.com	Frankfurt am Main, Hessen, Germany	The Constant Company, LLC (AS20473)	Vultr Holdings, LLC (hosting)

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
php2shell.pentest-ground.com	A	IPv4 address	45.77.55.213

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
22	open	ssh	-	-
443	open	https	-	-

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 443/tcp

UNCONFIRMED

Software / Version	Category
PHP 8.2.34	Programming languages
Debian	Operating systems
Apache HTTP Server 2.4.69	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 (10)

Port 22

✔ Scanned for version-based vulnerabilities

Port 443

- ✔ Checked for "PHP2Shell - Remote Code Execution (CVE-2026-109618 & CVE-2026-109619)"
- ✔ Scanned for vulnerabilities in PHP
- ✔ 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:	php2shell.pentest-ground.com
Preset:	Custom
Scanning engines:	Version_based, Nuclei
Check alive:	True
Extensive modules:	False
Protocol type:	TCP
Ports to scan:	Top 1000 ports
CVEs:	CVE-2026-109618
Requests per second:	-
Scan CISA KEV only:	-
Fast mode:	-