



PHP2Shell Remote Code Execution Vulnerabilities

Critical PHP vulnerabilities could allow unauthenticated remote code execution, prompting emergency security updates and urgent patching.

<https://www.php.net/archive/2026.php#2026-10-20-1>

CVEs: [CVE-2026-109618](#), [CVE-2026-109619](#), [CVE-2026-115560](#)

Successful exploitation could allow attackers to execute arbitrary code within the PHP application process, potentially compromising the affected server and exposing sensitive data, application files, or connected databases, depending on the process privileges and system configuration.

FortiGuard Labs is monitoring the PHP2Shell vulnerabilities and related threat activity. Updates will be provided as new threat intelligence emerges and additional protections become available. Organizations are advised to apply the relevant security updates and consult the FortiGuard coverage information for the latest protection status.

Background

PHP is an open-source, server-side scripting language widely used to build dynamic websites and web applications. It powers content management systems, e-commerce platforms, and other web services, including WordPress, which relies on PHP to run its core functionality. According to W3Techs, as of October 21, 2026, PHP was used by 69.3% of websites whose server-side programming language is known.

Because PHP is deployed across a large portion of the web, vulnerabilities in its underlying runtime can affect many different applications and hosting environments. The PHP2Shell vulnerabilities are particularly serious because successful exploitation could allow unauthenticated attackers to execute arbitrary code on vulnerable servers, potentially exposing sensitive data and enabling further compromise. The broad use of PHP makes timely patching and identifying vulnerable deployments especially important.

CVE-2026-109618 - RCE via out-of-memory corruption: An out-of-memory condition can interrupt PHP while internal request data is only partially initialized. Subsequent request-cleanup operations may incorrectly process this invalid data, potentially enabling remote code execution.

CVE-2026-109619 - RCE via stale global state: Internal request state can persist after its associated memory has been freed. A later request handled by the same worker may access this stale state before normal initialization resets it, potentially enabling remote code execution.

PHP announced emergency security updates for October 21, 2026, following reports that details of the vulnerabilities had leaked ahead of the planned disclosure. Subsequent reports highlighted ongoing exploit research and potential attack activity, underscoring the urgency of applying the available patches. However, widespread exploitation of either vulnerability has not been independently confirmed.

On October 23, 2026, the PHP project published an informational advisory regarding the session upload-progress feature. The advisory recommends setting `session.upload\_progress.enabled=0` until the next regular bug-fix release to mitigate an unlikely remote code execution (RCE) vector tracked as CVE-2026-115560.

Latest Developments

FortiGuard Labs recommends a defense-in-depth approach to reduce exposure to attacks targeting vulnerable PHP deployments and is currently monitoring the situation and will provide updates as new information becomes available and additional protections are released. Organizations should prioritize patching internet-facing PHP servers and other exposed deployments immediately. Apply the security updates. Upgrade to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35, as appropriate. Organizations using vendor-maintained packages should apply the corresponding security updates from their distributions or service providers.

October 23, 2026: PHP has disclosed an additional, configuration-dependent remote code execution vulnerability, CVE-2026-115560, and recommends a temporary mitigation while a fix is pending.

<https://thehackernews.com/2026/10/urgent-php-warns-of-another-unpatched.html>

October 23, 2026: FortiGuard Labs provides virtual patching and guidance to help organizations safely address critical PHP vulnerabilities.

<https://www.fortinet.com/blog/industry-trends/understanding-php2shell-vulnerabilities-and-reducing-risk-while-you-patch>

October 21, 2026: PHP published details of both critical remote code execution vulnerabilities and released security updates for PHP 8.5.12, 8.4.27, 8.3.36, and 8.2.35. Government cybersecurity agencies also issued advisories urging organizations to patch.

<https://www.php.net/archive/2026.php#2026-10-20-1>

October 21, 2026: Additional threat intelligence reporting detailed exploitation attempts, public proof-of-concept research, and mitigation guidance. Organizations were advised to prioritize patching internet-facing PHP deployments.

<https://www.fortiguard.com/threat-signal-report/6551/php2shell-remote-code-execution-vulnerabilities>

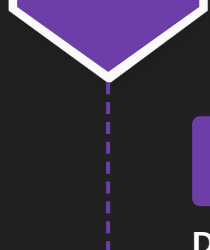
October 20, 2026: Details of CVE-2026-109618 and CVE-2026-109619 circulated publicly ahead of the planned disclosure, prompting PHP to advance its security release.

October 17, 2026: Amazon Threat Intelligence identified an exploitation attempt targeting PHP2Shell in its MadPot telemetry, dated four days before public disclosure.

<https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot>

August 01, 2026: Calif identified a vulnerability through AI-assisted source-code analysis and later reported the first flaw to the PHP project.

<https://calif.io/php2shell/>

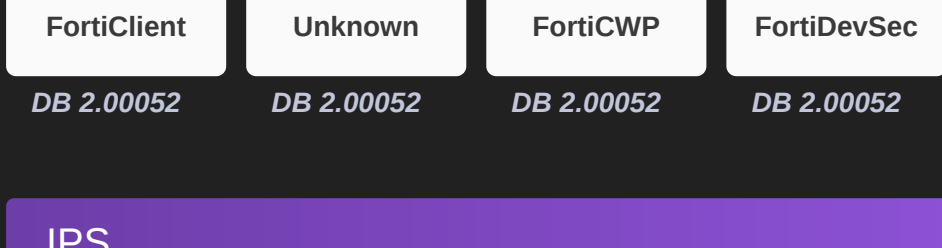


PROTECT

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

Vulnerability

Detects end-user devices running the vulnerable application.



DB 2.00052

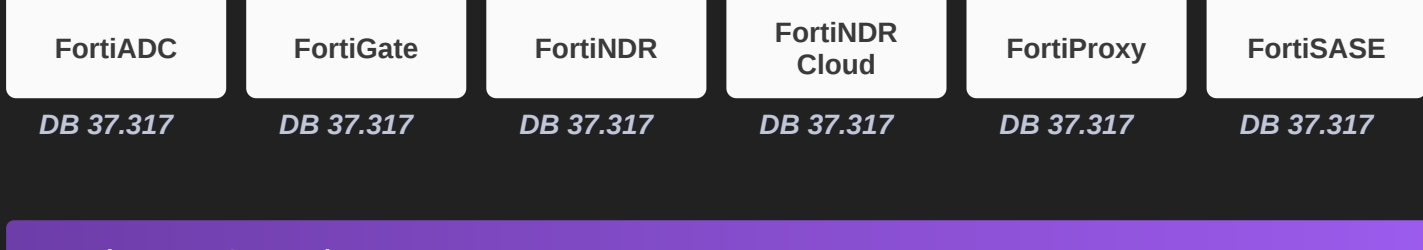
DB 2.00052

DB 2.00052

DB 2.00052

IPS

Detects and blocks attack attempts leveraging the vulnerability



DB 37.317

DB 37.317

DB 37.317

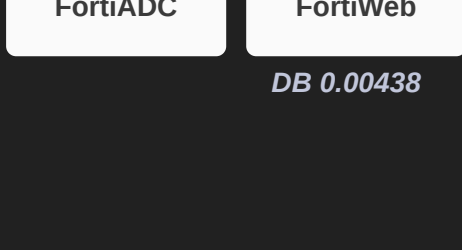
DB 37.317

DB 37.317

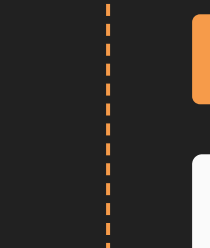
DB 37.317

Web App Security

Detects and blocks attack attempts leveraging the vulnerability



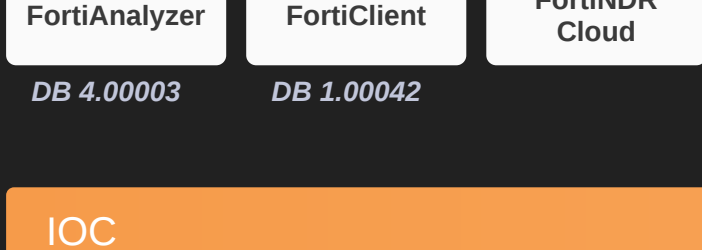
DB 0.00438



DETECT

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

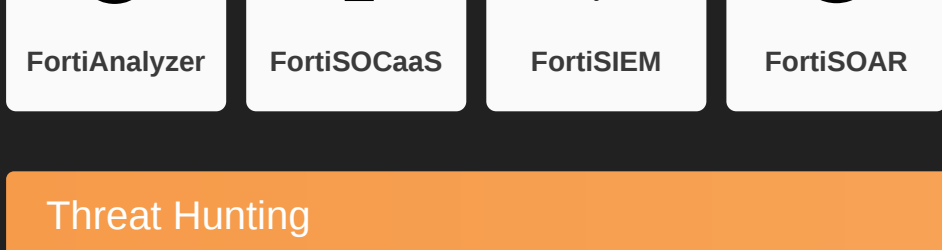
Outbreak Detection



DB 4.00003

DB 1.00042

IOC



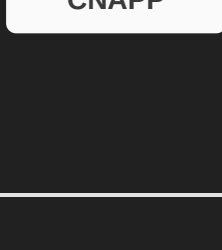
FortiAnalyzer

FortiSOCaaS

FortiSIEM

FortiSOAR

Threat Hunting

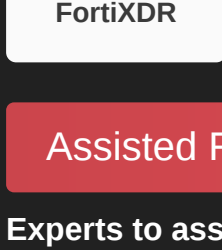


RESPOND

Develop containment techniques to mitigate impacts of security events:

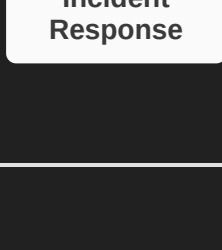
Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

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

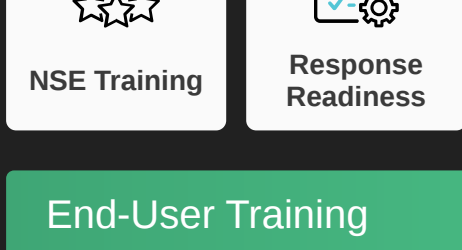


RECOVER

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.

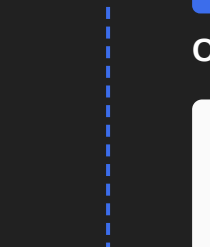
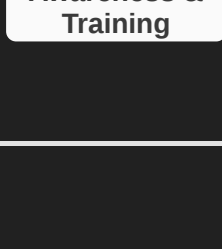


NSE Training

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.

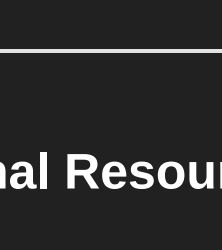


IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

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



Additional Resources

Amazon Threat Intelligence <https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot>

Fortinet Blog <https://www.fortinet.com/blog/industry-trends/understanding-php2shell-vulnerabilities-and-reducing-risk-while-you-patch>

PHP Fixes <https://phpnews.net/php-critical-vulnerabilities>

21 Oct 2026 Security advisory <https://www.php.net/>

Usage statistics of PHP (W3 Tech Survey) <https://w3techs.com/technologies/comparison/pl-js%2Cpt-PHP>

Learn more about [FortiGuard Outbreak Alerts](#)