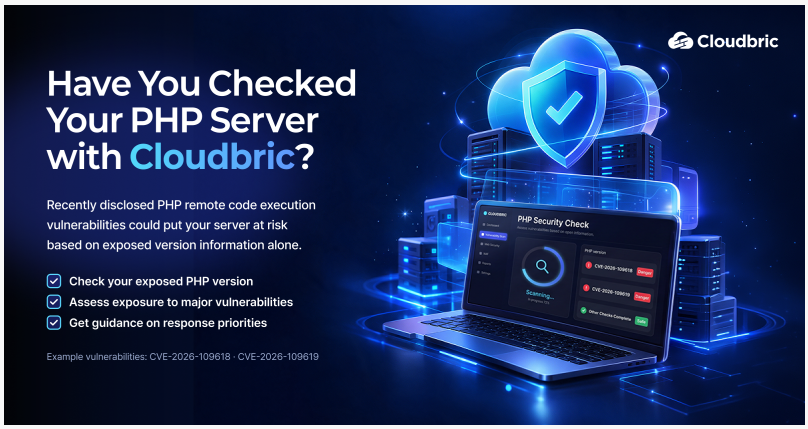
Penta Security Launches Website Security Check and Response Rules for PHP2Shell Vulnerabilities

· Check PHP vulnerability exposure by entering a website URL and expanded PHP2Shell support with WAPPLES and Cloudbric WAF+ response rules



SEOUL, SOUTH KOREA, October 26, 2026 /EINPresswire.com/ -- Cybersecurity company Penta Security has launched the Cloudbric Security Check service in response to the recently disclosed PHP remote code execution vulnerabilities known as 'PHP2Shell'. The service enables organisations to check whether their websites are exposed to the vulnerabilities and provides guidance on appropriate remediation measures for their environments.

Cloudbric Security Check requires no software installation. Users simply enter a website URL to identify the PHP version exposed externally and assess whether the website may be affected by major vulnerabilities. Based on the results, the service provides the necessary response measures and their order of priority. The service is available to anyone and can be accessed through the Penta Security and Cloudbric websites.

The service uses a non-intrusive assessment method that checks server response information without attempting to exploit the vulnerabilities, and provides results within seconds. It can be accessed through the Penta Security and Cloudbric websites and is available to anyone.

For websites where the PHP version cannot be identified through the website check alone, Penta Security also provides an assessment script that allows users to check the PHP version installed on the server and related configuration settings directly. Based on the assessment results, users can review appropriate response measures for their operating environment, including updates and temporary mitigation measures. The service is available in English, Korean and Japanese.

Immediately after the vulnerabilities were disclosed, Penta Security distributed custom rules and

configuration guidance to WAPPLES intelligent web application firewall customers to help defend against attacks exploiting the PHP vulnerabilities. The company also applied the relevant response rules to its SaaS-based web security service, Cloudbric WAF+.

PHP2Shell refers collectively to the PHP remote code execution vulnerabilities CVE-2026-109618 and CVE-2026-109619, which can be exploited without authentication. The fundamental response is to update to a PHP version in which the vulnerabilities have been fixed. Where immediate patching is difficult, organisations can use a web application firewall to block requests that attempt to exploit the vulnerabilities, helping to mitigate risk until the patch can be applied.

Jihae Lee, CCO (Chief Compliance Officer) of Penta Security, said, “As AI and automation technologies accelerate vulnerability analysis and attacks to unprecedented levels, organisations must ensure that their security response can keep pace. We hope that organisations which find it difficult to immediately determine their PHP operating environment and exposure to these vulnerabilities can use the Cloudbric Security Check site to quickly understand their current exposure, identify the necessary response measures and proceed with appropriate action.”

Penta Security Inc.
Penta Security Inc

This press release can be viewed online at: https://www.einpresswire.com/article/952260073

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.