HC3: Sector Alert

June 12, 2024 TLP:CLEAR Report: 202406121500

Critical Vulnerability in PHP Programming Language

Overview

Administrators are being advised to update their systems following the disclosure of a critical remote code execution vulnerability in PHP. PHP, or Hypertext Preprocessor, is a widely used open-source scripting language that is used to create dynamic web pages and applications on both Windows and Linux servers. It is a general-purpose language that can be embedded into HTML, which makes it popular with developers because it simplifies HTML code. The vulnerability, discovered on May 7, 2024, and now tasked as CVE-2024-4577, impacts all releases since version 5.x, potentially impacting a massive number of servers worldwide. This Sector Alert provides an overview of the vulnerability and remediation strategies.

Report

The CVE-202404577 vulnerability affects all versions of PHP running on a Windows device. That includes version branches 8.3 prior to 8.3.8, 8.2 prior to 8.2.20, and 8.1 prior to 8.1.29. The 8.0, 7, and 5 version branches are also vulnerable, but because they are no longer supported, admins will have to follow mitigation advice since patches are not available.

The vulnerability is actually a recurrence of an argument injection bug that was patched more than a decade ago. In 2012, while implementing PHP, an overlooked Best-Fit feature of encoding conversion within the Windows operating system allowed unauthenticated attackers to bypass the previous protecton of CVE-2012-1823 by specific character sequences.

The newly discovered vulnerabulity occurs when a server of PC is running in certain configurations that expose Common Gateway Interface (CGI), which enables web servers to execute an external program to process HTTP or HTTPS user requests. This means that when PHP is configured to allow certain types of CGI interaction, arbitrary arguments can be injected remotely. This, in turn, would allow a potential attacker to trigger code execution on the targeted server and take complete control.

CVE-2024-4577 affects PHP only when it runs in CGI mode, in which a web server parses HTTP requests and passes them to a PHP script for processing. Even when PHP is not set to CGI mode, however, the vulnerability may still be exploitable when PHP executables such as php.exe and php-cgi.exe are in directories that are accessible by the web server. This configuration is set by default in XAMPP for Windows, making the platform vulnerable unless it has been modified.

The researcher credited with discovering this vulnerability stated that while it is difficult to assess whether a machine is vulnerable to the attack scenario, some systems are more vulnerable than others. While Windows systems running Japanese, traditional Chinese, or simplified Chinese are all presumed to be vulnerable, the danger for other systems depends on whether CGI mode is enabled or the PHP binary is exposed. For Windows running in other locales such as English, Korean, and Western European, due to the wide range of PHP usage scenarios, it is currently not possible to completely enumerate and eliminate all potential exploitation scenarios.

Despite only being discovered a few days ago, cybersecurity researchers have already confirmed detected exploitation attempts involving the flaw against its honeypot servers within 24 hours of public disclosure of the vulnerability. As with any critical vulnerability impacting many devices, once disclosed, both threat actors and researchers immediately began attempting to find vulnerable systems.

HC3: Sector Alert

June 12, 2024 TLP:CLEAR Report: 202406121500

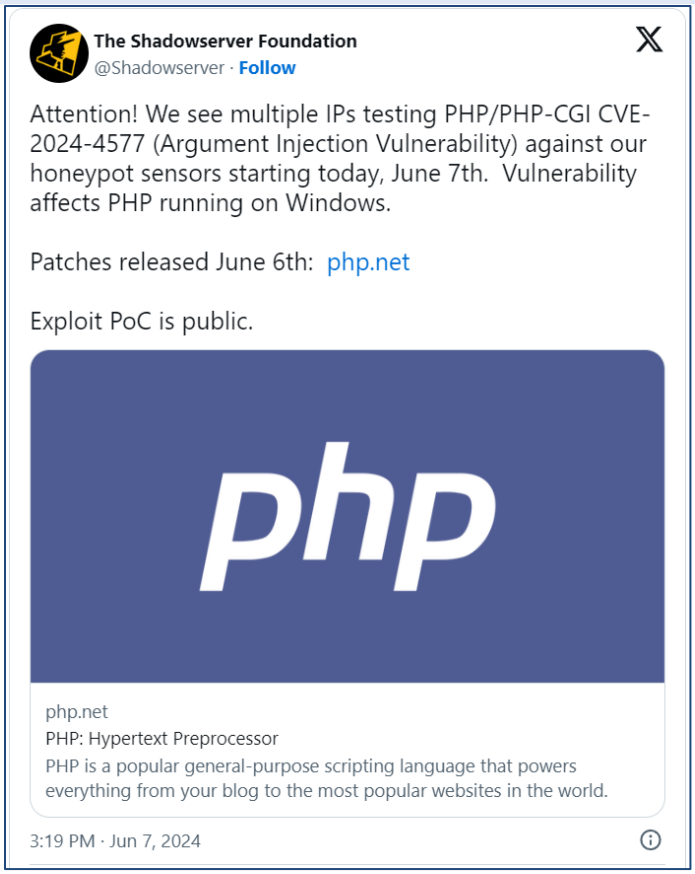

Figure 1: Cybersecurity company's posting on the X social media platform, highlighting multiple IP addresses scanning for vulnerable servers. *(Source: BleepingComputer)*

Defense and Mitigations

Because assessing whether a system is vulnerable can be difficult, researchers recommend simply updating the PHP installation to the latest version, 8.3.8. For systems that cannot be immediately upgraded, and for users of EoL versions, it is recommended to apply a mod_rewrite rule to block attacks, like the following:

```
RewriteEngine On
RewriteCond %{QUERY_STRING} ^%ad [NC]
RewriteRule .? – [F,L]
```

If you use XAMPP and do not need the PHP CGI feature, find the 'ScriptAlias' directive in the Apache configuration file (typically at 'C:/xampp/apache/conf/extra/httpd-xampp.conf') and comment it out.

Admins can determine if they use PHP-CGI using the phpinfo() function and checking the 'Server API' value in the output.

Additionally, administrators should consider moving away from the outdated PHP CGI altogether and opt for a more modern solution, such as Mod-PHP, FastCGI, or PHP-FPM.

In Windows, a locale is a set of user preference information related to the user's language, environment,

and/or cultural conventions. As of June 7, 2024, researchers have only tested three locales that are now confirmed as vulnerable. Researchers have not yet tested other locales due to the wide range of PHP usage scenarios in locales such as English, Korean, and Western European. As such, they urge people using them to perform a comprehensive asset assessment to test their usage scenarios.

National Vulnerability Database

CVE-2024-4577 (Last Modified June 10, 2024)				
Description	Vulnerability	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use “Best-Fit” behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.		
	CVSS Score	N/A (NVD assessment not yet provided)		
Weakness Enumeration	CWE-ID	CWE-78		
	CWE Name	Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)		
	Source	NIST		
Known Affected Software Configurations	Configuration 1	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	From (including) 5.0.0	Up to (excluding) 8.1.29
	Configuration 1	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	From (including) 8.2.0	Up to (excluding) 8.2.20
	Configuration 1	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	From (including) 8.3.0	Up to (excluding) 8.3.8

References to Advisories, Solutions, and Tools	
Hyperlink	Resource
https://arstechnica.com/security/2024/06/php-vulnerability-allows-attackers-to-run-malicious-code-on-windows-servers/	Exploit Third Party Advisory
https://blog.orange.tw/2024/06/cve-2024-4577-yet-another-php-rce.html	Third Party Advisory
https://cert.be/en/advisory/warning-php-remote-code-execution-patch-immediately	Third Party Advisory
https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/	Exploit Third Party Advisory
https://github.com/11whoami99/CVE-2024-4577	Exploit
https://github.com/php/php-src/security/advisories/GHSA-3qgc-jrrr-25jv	Broken Link
https://github.com/rapid7/metasploit-framework/pull/19247	Exploit
https://github.com/watchtowrlabs/CVE-2024-4577	Exploit Third Party Advisory
https://github.com/xcanwin/CVE-2024-4577-PHP-RCE	Exploit Third Party Advisory
https://isc.sans.edu/diary/30994	Exploit Third Party Advisory
https://labs.watchtowr.com/no-way-php-strikes-again-cve-2024-4577/	Exploit Third Party Advisory
https://www.imperva.com/blog/imperva-protects-against-critical-php-vulnerability-cve-2024-4577/	Third Party Advisory
https://www.php.net/ChangeLog-8.php#8.1.29	Release Notes
https://www.php.net/ChangeLog-8.php#8.2.20	Release Notes
https://www.php.net/ChangeLog-8.php#8.3.8	Release Notes

Way Forward

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities, and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with the tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

References

"CVE-2024-4577 Detail." National Institute of Standards and Technology – National Vulnerability Database. June 10, 2024. https://nvd.nist.gov/vuln/detail/CVE-2024-4577#toggleConfig1

Goodin, Dan. "Nasty bug with very simple exploit hits PHP just in time for the weekend." Ars Technica. June 7, 2024. https://arstechnica.com/security/2024/06/php-vulnerability-allows-attackers-to-run-malicious-code-on-windows-servers/

"New PHP vulnerability Exposes Windows Servers to Remote Code Execution." The Hacker News. June 8, 2024. https://thehackernews.com/2024/06/new-php-vulnerability-exposes-windows.html

Nichols, Shaun. "PHP updates urged over critical vulnerability that could lead to RCE." SC Media. June 7, 2024. https://www.scmagazine.com/news/php-updates-urged-over-critical-vulnerability-that-could-lead-to-rce

Toulas, Bill. "PHP fixes critical RCE flaw impacting all versions for Windows." BleepingComputer. June 7, 2024. https://www.bleepingcomputer.com/news/security/php-fixes-critical-rce-flaw-impacting-all-versions-for-windows/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

HC3: Sector Alert

June 12, 2024 TLP:CLEAR Report: 202406121500

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback