Alert Bulletin

Bulletin N.: 2024-16
Publication Date: 12/06/2024
Subject: Alert 2024-16 RCE Vulnerability in PHP CGI on Windows Systems
Traffic Light Protocol (TLP): White

Affected Product(s):

- The vulnerability **CVE-2024-4577** affects all versions of PHP installed on Windows systems:
- PHP 8.3 < 8.3.8
- PHP 8.2 < 8.2.20
- PHP 8.1 < 8.1.29

The PHP branches **8.0**, **7**, and **5** are at **End of Life (EOL)** and no longer receive maintenance.

Description:

On **June 6, 2024**, the security team at **DEVCORE** alerted about a critical security vulnerability in the **PHP programming language**, specifically in installations on Windows. This vulnerability is designated as **CVE-2024-4577**, with a severity score of **9.8** (Critical).

In the listed versions of PHP, when using **Apache** and **PHP-CGI** on Windows, if the system is configured to use certain code pages, Windows may utilize the "Best-Fit" behavior to replace characters in the command line provided to Win32 API functions. The PHP CGI module may misinterpret these characters as PHP options, potentially allowing a malicious actor to pass options to the executing PHP binary, thereby revealing the source code of scripts or executing arbitrary PHP code on the server (RCE), among other risks.

There are two vulnerable configuration scenarios:

1. **Running PHP in CGI Mode**
   When configuring the **Action Directive** to assign corresponding HTTP requests to an executable PHP-CGI binary on the Apache HTTP server, this vulnerability can be directly exploited. Common affected configurations include: **Configuration A**

```
AddHandler cgi-script .php
Action cgi-script "/cgi-bin/php-cgi.exe"
```

Configuration B

```
<FilesMatch "\.php$">
SetHandler application/x-httpd-php-cgi
```

```
</FilesMatch>
Action application/x-httpd-php-cgi "/php-cgi/php-cgi.exe"
```

2. **Exposing the PHP Binary** – Default Configuration in XAMPP
   If PHP is not configured in CGI mode, this vulnerability is also affected by simply exposing the executable PHP binary in the CGI directory. Common scenarios include:

- Copying either **php.exe** or **php-cgi.exe** to the **/cgi-bin/** directory.
- Exposing the PHP directory using the **ScriptAlias** directive, such as:

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

It is important to note that the second scenario is the default configuration of **XAMPP for Windows**, meaning all versions of XAMPP installations on Windows are vulnerable by default at the time of this bulletin's publication. The XAMPP team itself advises against using the free version on production servers.

Apache Friends FAQ

Recently, several exploits and PoCs for this vulnerability have been made public, significantly increasing the likelihood of exploitation. There are also reports of ransomware groups exploiting this vulnerability in their campaigns (such as "TellYouThePass").

On **Shodan**, it can be observed that there are approximately **1456 vulnerable devices** in Mexico alone.

Impact:

A malicious actor who may already be inside the network could exploit this vulnerability to partially or completely delete backups, thereby preventing recovery from a backup.

Mitigation:

For systems that cannot be updated, the following instructions can be used to temporarily mitigate the vulnerability:

For users unable to update PHP, the following rewrite rules can be used to block attacks. Please note that these rules are only a temporary mitigation for regional configurations of **Traditional Chinese**, **Simplified Chinese**, and **Japanese**:

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

For users using **XAMPP for Windows**, whose development team has not yet released the corresponding update files for this vulnerability at the time of writing this bulletin, if you confirm that you do not need the PHP CGI feature, you can avoid exposure to the vulnerability by modifying the following configuration in the Apache HTTP server:

```
C:/xampp/apache/conf/extra/httpd-xampp.conf
```

Within the file, comment out the line corresponding to:

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

However, since PHP CGI is an outdated architecture, it is recommended to consider migrating to a more secure architecture such as **Mod-PHP**, **FastCGI**, or **PHP-FPM**.

Solution:

All users are advised to update to the latest versions of PHP **8.3.8**, **8.2.20**, and **8.1.29**. The official download link is:

Download PHP