Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

PHP RCE Flaw Opens a Gateway for TellYouThePass Ransomware

Date of Publication	Admiralty Code	TA Number
June 12, 2024	A1	TA2024227

Summary

First Seen: May 6, 2024
Affected Product: Windows
Malware: TellYouThePass ransomware
Impact: A critical security flaw in PHP impacts all versions installed on Windows operating systems. The TellYouThePass ransomware gang is actively exploiting this vulnerability, leading to arbitrary code execution on affected servers and potentially compromising entire systems. This flaw poses significant risks to PHP-based web applications.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-4577	PHP-CGI Argument Injection Vulnerability	PHP version: 5 - 8.3.7	✗	✗	✓

Vulnerability Details

#1 A critical security flaw in PHP has been identified, which can be exploited to achieve remote code execution. The PHP-CGI Argument Injection Vulnerability, designated as CVE-2024-4577, affects all versions of PHP installed on Windows operating systems. Furthermore, all XAMPP a popular PHP development environment, on Windows are inherently vulnerable when configured to use locales prone to this encoding conversion flaw, including Traditional Chinese, Simplified Chinese, or Japanese.

#2 The CVE-2024-4577 vulnerability stems from an error in handling character encoding conversions, specifically the 'Best-Fit' feature on Windows when PHP operates in CGI mode. As of June 9, 2024, there are approximately 458,800 potentially vulnerable PHP instances, predominantly in the U.S. and Germany.

#3

Since June 8, 2024, the TellYouThePass ransomware gang has been exploiting this recently patched CVE-2024-4577 vulnerability to execute remote code and deploy a .NET variant of their file-encrypting malware on target systems. The initial infection vector involves an HTA file containing a malicious VBScript. When decoded, this script reveals binary data loaded into memory during runtime. This vulnerability, resulting from improper input validation, poses significant risks to web applications built with PHP.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4577	PHP versions: 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Upgrade PHP Versions: It is strongly recommended that all users upgrade to the latest PHP versions, including 8.3.8, 8.2.20, and 8.1.29. These updates likely contain patches and fixes for known vulnerabilities, enhancing the security of your PHP installations.

End-of-Life PHP Versions: Since PHP 8.0, PHP 7, and PHP 5 are End-of-Life (EOL) and no longer maintained, it's crucial to migrate away from these versions to ensure continued security support. Consider upgrading to supported PHP versions as soon as possible to mitigate security risks.

Implement Mod_Rewrite Rules: For systems that cannot be immediately upgraded or for users of EOL PHP versions, temporarily mitigating by applying a mod_rewrite rule to block attacks is advisable. Utilize the provided example rule to enhance security by blocking potentially malicious requests.

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

Review XAMPP Configuration: If you use XAMPP and do not require the PHP CGI feature, consider disabling it by commenting out the 'ScriptAlias' directive in the Apache configuration file. This action can help reduce the attack surface and mitigate potential vulnerabilities associated with PHP CGI.

Verify PHP-CGI Usage: Admins can determine if they are using PHP-CGI by utilizing the phpinfo() function and checking the 'Server API' value in the output. If PHP-CGI is detected, consider migrating to more secure alternatives such as FastCGI, PHP-FPM, or Mod-PHP to enhance server security and performance.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0040 Impact
T1587 Develop Capabilities	T1059 Command and Scripting Interpreter	T1587.001 Malware	T1608 Stage Capabilities
T1588.006 Vulnerabilities	T1204.002 Malicious File	T1036 Masquerading	T1027.009 Embedded Payloads
T1082 System Information Discovery	T1105 Ingress Tool Transfer	T1659 Content Injection	T1190 Exploit Public-Facing Application
T1543 Create or Modify System Process	T1055 Process Injection		

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[:]/88[.]218[.]76[.]13/dd3[.]hta
IPv4	88[.]218[.]76[.]13

TYPE	VALUE
SHA256	95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3, 5a2b9ddddea96f21d905036761ab27627bd6db4f5973b006f1e39d4acb04a618, 9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53
Bitcoin Address	bc1qnuxx83nd4keeegrumtnu8kup8g02yzgff6z53l
File Name	dd3.hta

Patch Details

Upgrade to the latest patched PHP versions 8.3.8, 8.2.20, and 8.1.29 is highly recommended.

Link:
https://www.php.net/downloads

References

https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability-en/

https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware

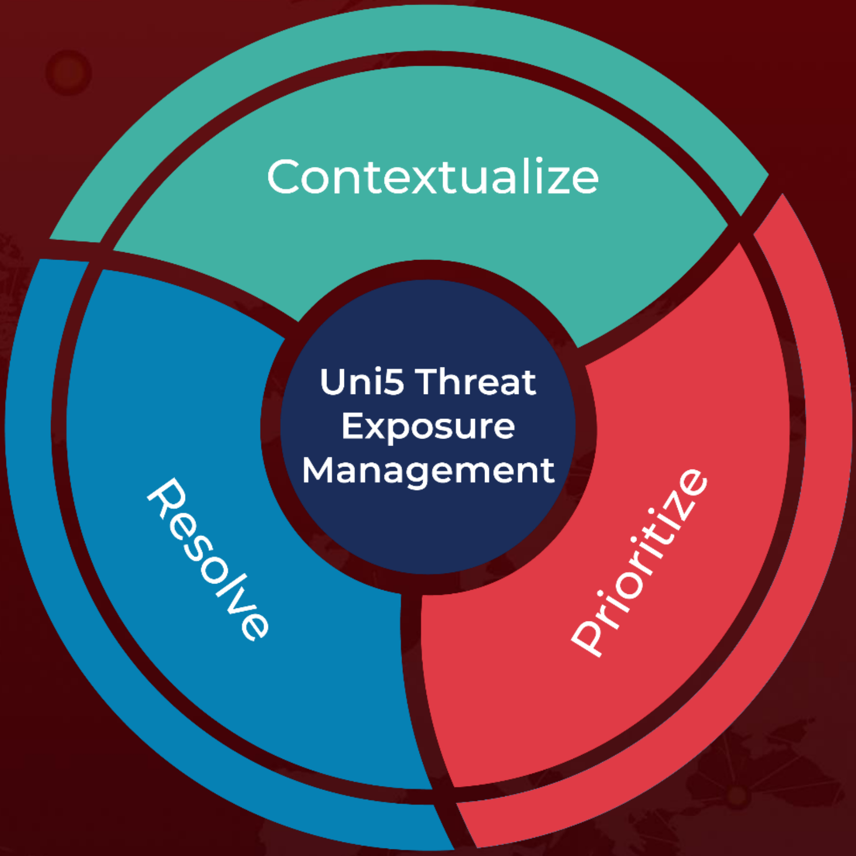
https://github.com/watchtowrlabs/CVE-2024-4577

https://www.hivepro.com/threat-advisory/ransomware-threats-exploit-cve-2023-46604-in-apache-activemq-servers/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 12, 2024 • 6:30 AM

More at www.hivepro.com