PHP-CGI Remote Code Execution Vulnerability Under Mass Exploitation

Overview

Devcore, a cybersecurity firm, reports that threat actors are actively exploiting CVE-2024-4577 (CVSS 9.8) - an RCE vulnerability in Windows servers running PHP-CGI with Apache. The flaw allows unauthenticated attackers to execute arbitrary code by injecting malicious arguments, leading to full system compromise.

CVE-2024-4577 is a PHP-CGI argument injection vulnerability impacting Windows systems with PHP running in CGI mode. The flaw stems from PHP's improper handling of Unicode character conversion, where specific sequences can be misinterpreted as PHP options by the php-cgi module.

Affected Products

- All PHP versions on Windows prior to the patched versions:
  - PHP 8.1.29
  - PHP 8.2.20
  - PHP 8.3.8
- Servers running Apache with PHP-CGI configured to use vulnerable code pages.

This issue was publicly disclosed in June 2024, and a proof-of-concept (PoC) exploit was released within 24 hours. Attackers (including TellYouThePass ransomware gang) have since automated exploitation attempts. Attackers are scanning for vulnerable systems worldwide and deploying malware, ransomware, and adversarial tools to maintain persistence and escalate privileges.

CVE-2024-4577 has been leveraged to deploy ransomware and steal credentials. Initial reports focused on Japan, but exploitation has expanded globally. There has been a spike in activity in the US, UK, Singapore, Indonesia, Taiwan, Hong Kong, India, Spain, and Malaysia since January 2025. Organizations using vulnerable PHP-CGI configurations are at risk and need to patch immediately.

Aspire Protects

- **Patch** – Upgrade to PHP 8.1.29, 8.2.20, or 8.3.8 immediately.
  - For those who cannot update, please see Devcore's recommended mitigations.
- Disable PHP-CGI if Not Needed – Restrict PHP-CGI execution or transition to more secure deployment methods.
- Monitor for Exploitation Attempts – Look for abnormal PHP arguments and unauthorized PHP-CGI processes.
- Use Web Application Firewalls (WAFs) – Implement rules to detect and block exploit attempts.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have targeted vulnerable PHP-CGI instances to gain access.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – The attacker bypassed restrictions to gain SYSTEM privileges.

Persistence

- Create or Modify System Process [T1543.003] – The attacker created malicious services to maintain access.

Credential Access

- OS Credential Dumping [T1003] – The attacker may have attempted to extract credentials post-compromise.

IoCs

- Unusual php-cgi.exe execution with unexpected arguments.
- Unauthorized registry modifications and scheduled tasks.
- Cobalt Strike activity using the TaoWu plugin.
- IP Addresses – Significant exploit traffic observed from Germany, China, US, and other regions.

There are no other known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerability may impact the following industries/sectors:

- Finance
- Ecommerce
- Healthcare
- Government
- Manufacturing
- Retail
- Energy
- Education
- Telecommunications
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current

security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Unmasking the new persistent attacks on Japan

Security Alert: CVE-2024-4577 - PHP CGI Argument Injection Vulnerability | DEVCORE

VU#520827 - PHP-CGI query string parameter vulnerability