Wilcompute
IT TECHNOLOGIES

October 27, 2026 By: Ronald Wilson

Name: PHP2Shell

Versions: 8.2.34 | 8.3.35 | 8.4.26 | 8.5.11 and below

CVE: CVE-2026-109618, CVE-2026-109619

Type: Remote Control Execution

Exploited: Successful exploit via public

How to Fix:

Patches have been released for CVE-2026-109618 and CVE-2026-109619. Recommended versions should be updated to 8.4.27, 8.3.36, 8.2.35, and 8.5.12. (Apache mod_php, PHP-FPM, php-cgi, FrankenPHP and LiteSpeed)

The patch removes longjmp() for OOM, avoiding an early exit out of contexts that do not properly account for it. It is replaced with a delayed, graceful soft OOM triggered at the next VM safe point, and an immediate hard OOM using _exit() if memory consumption reaches a second, higher threshold. The shutdown procedure will no longer see invalid state, and PHP's normal ability to limit memory consumption is retained (Zelenka, 2026)[i]

to help detect the presence of the PHP2Shell RCE vulnerability, Cybersecurity and Infrastructure Security Agency (CISA) released SIGMA detection rules on October 23, 2026.

Warning...

Updating to a PHP release containing the patch to this vulnerability is the *only* complete mitigation.

History:

During an analysis of the CVE-2026-109618 and 2026-109619, an uninitialized pointer was discovered and maliciously used via a remote attack.

During an established session with a website running PHP 5 version 8.2.34 | 8.3.35 | 8.4.26 | 8.5.11 and below, a configuration file contains the entry session.upload_progress.enabled=On which interacts with the function longjmp(). The function is utilized to identify out-of-memory (OOM) errors, exit the current context, and abort handling of the request, once a maximum limit of requests are reached (VulDB, 2026)[ii].

Some contexts may not account for this exit and leave request of memory in an uninitialized state before granting the allocated request of memory. The request cleanup procedure may read or branch (redirect) from this memory after multiple OOM triggers, creating a vulnerable state where a remote code execution (RCE) can be inserted, executed, and connection established.

How:

Multiple requests are quickly received and consumed in memory until its' maximum limit is reached. (i.e. massive file uploads) The program immediately calls the function longjmp() and executes a request shutdown function from the memory stack.

Executing the shutdown function bypasses local cleanup and initialization of code, therefore leaving memory in a volatile, uninitialized, or dangling state.

Before an established session reaches an OOM state an attacker is able to manipulate the heap and execute malicious code such as sending empty or malicious instrutions to the uninitialized state of memory. A pointer is created to execute malicious payload in memory.

In an active session the function php_request_shutdown is executed and PHP resources free active memory. When an uninitialized memory space is left behind the longjmp() function interrupt and jumps to an executing branch in memory where a function pointer such as a destructor can be used to corrupt memory, by executing the attackers payload and establishing an RCE connection (Akamai Security Intelligence Group, October 2026)[iii]

Discovery in the Wild:

According to Adel Karimi of Perplixity, malicious events were recorded after detecting activity of remote code execution via a honeypot. The malware was executed against an Apache mod_php with version PHP 8.4.26 (Gatlan, October 2026)[iv]

The payload contained an 800 KiB decoded cookie dump, and a function address using a public exploit's offset.

Company's including Cloudflare, Hadrian, watchtower, Previdian, and Patchstack have all detected unsuccessful attempts using PHP2Shell vulnerability as an exploit.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. WilcomputeIT Technologies does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by WilcomputeIT Technologies.

References

[i] Jakub Zelenka, “RCE via OOM connection” (October 2026). https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

[ii] “PHP UP TO 8.2.34/8.3.35/8.4.26/8.5.11 LONGJMP PHP2SHELL UNINITIALIZED POINTER” (October 2026). https://vuldb.com/vuln/424813

[iii] Akamai Security Intelligence Group, “Understanding PHP2Shell: Everything You Need to Know”, October 2026. https://www.akamai.com/blog/security-research/understanding-php2shell-everything-you-need-to-know

[iv] Sergiu Gatlan, “PHP2Shell Security Flaws Now Successfully Exploited In the Wild”

(https://www.bleepingcomputer.com/news/security/php2shell-security-flaws-now-sucessfully-exploited-in-the-wild/)