

PHP to Issue Emergency Release for Two Critical Remote Code Execution Flaws



PHP will publish an out-of-cycle release on October 21 at 14:00 UTC for two critical flaws rated 9.2 on CVSS v4.0. watchTowr says both allow remote code execution; no exploitation has been reported.

- Two critical PHP vulnerabilities are rated 9.2 on CVSS v4.0 by the PHP security team.
- The fix arrives in an out-of-cycle release at 14:00 UTC on October 21.
- watchTowr researchers say the flaws allow remote code execution.
- Only branches 8.2 through 8.5 can receive the fix.
- No exploitation has been reported so far, and technical details have not been published.

What has been announced

The PHP project will release an out-of-cycle security update at 14:00 UTC on October 21 to address two vulnerabilities its security team rates 9.2 on the CVSS v4.0 scale. The team has not described the flaws publicly.

Researchers at watchTowr, who have named the issue PHP2Shell, say both vulnerabilities allow **remote code execution**. No exploitation has been reported so far.

Who can receive the fix

Only the four supported branches, PHP 8.2 through 8.5, can receive the patch. Systems running older branches are not covered by this release, according to the source, so any such deployments will need a separate plan.

What this means for institutions

Because details are limited, the practical priority is readiness rather than reaction. Once the release is published, teams that run PHP in web applications, portals or internal tools should be able to identify which systems are affected and update them quickly. Since technical details may follow the release, the window between publication and any attempted exploitation could be short, though the source does not report any such activity.

Institutions should treat internet-facing PHP applications as the first priority and confirm that the versions they run fall within the supported branches.

What to do now

1. Inventory all systems and applications running PHP, including third-party and hosted ones, and record their branch versions.
2. Identify internet-facing PHP applications and prioritise them for patching once the release is published.
3. Plan an emergency change window for 21 October so the update can be tested and deployed without delay.
4. Flag any deployments on branches older than 8.2 and decide on an upgrade or compensating controls.
5. Increase monitoring of web server and application logs for unusual behaviour on PHP hosts.