PHP Vulnerability Response Checklist

A checklist for responding to the PHP security releases published on 19 November 2026 (8.5.13, 8.4.28, 8.3.37 and 8.2.36).

Date checked	Checked by	Servers / services covered
/ /		

1. Identify what is affected

Done	Item	Notes
☐	Listed every server and service running PHP (own servers, shared hosting, sites maintained by contractors, WordPress sites, etc.)	
☐	Checked the PHP version on each server (php -v, the hosting control panel, phpinfo, etc.)	
☐	Checked how PHP runs (PHP-FPM, PHP-CGI or a web server module)	
☐	Checked which extensions are in use (session, SOAP, PHAR, DOM, etc.)	
☐	Confirmed the maintenance contractor and their contact details	

2. Decide the target version

Branch	Fixed version	End of security support	Action
8.5	8.5.13 or later	31 Dec 2029	Update to the fixed version
8.4	8.4.28 or later	31 Dec 2028	Update to the fixed version
8.3	8.3.37 or later	31 Dec 2027	Update to the fixed version
8.2	8.2.36 or later	31 Dec 2026	Update, and plan a move to 8.3 or later
8.1 and earlier	None	Ended	Move to 8.3 or later

PHP packages shipped by Linux distributions may carry different version numbers from the table above. Check the distribution's security advisories to confirm that each CVE is fixed.

3. Update

Done	Item	Notes
☐	Backed up code, databases and configuration files before updating	

Done	Item	Notes
☐	Updated in a staging environment and checked the main screens and functions	
☐	Applied the update in production and restarted PHP-FPM and the web server	
☐	Confirmed the new version (both on the command line and for the PHP serving web requests)	
☐	Checked the error logs and main screens after the update	
☐	For hosting providers and contractors, confirmed when the update is scheduled and that it is done	

4. If you cannot update right away

Done	Item	Notes
☐	Made the PHP-FPM status page (pm.status_path) inaccessible from outside	
☐	Confirmed that PHP-CGI cannot be called directly from the web	
☐	Disabled unused extensions (SOAP, etc.)	
☐	Set an update date and shared it with those involved	

5. Record and report

Done	Item	Notes
☐	Recorded, for each target, the version before and after, what was done and the date	
☐	Reported to your manager and the person responsible for information security	
☐	Where needed, issued a notice to customers or users	

6. Prepare for next time

Done	Item	Notes
☐	Decided who checks vulnerability information and how often (php.net, JVN, distribution security advisories)	
☐	Turned this procedure into an internal manual and decided where it is kept and who revises it	

Reference: vulnerabilities fixed in the 19 November 2026 releases

CVE	Description	Branches
CVE-2026-115560	Session serializer mismatch can lead to remote code execution	8.2–8.5
CVE-2026-126714	Partially overwritten session files can lead to remote code execution	8.2–8.5
CVE-2026-129496	Timezone cache use-after-free can lead to remote code execution	8.2–8.5
CVE-2026-129474	Use-after-free in magic method backtraces can lead to remote code execution	8.5
CVE-2026-129291	PHP-FPM epoll use-after-free can lead to local privilege escalation	8.2–8.5
CVE-2026-129289	PHP-FPM request smuggling through an unread HTTP request body	8.2–8.5
CVE-2026-129292	PHP-FPM status endpoint XSS via unescaped user and script fields	8.2–8.5
CVE-2026-129538	PHP-CGI out-of-bounds read and write during PATH_INFO correction	8.2–8.5
CVE-2026-128090	PHAR OpenSSL signature bypass via algorithm downgrade	8.2–8.5
CVE-2026-128064	Mixed-case HTTPS and FTPS URLs can expose data in plaintext	8.2–8.5
CVE-2026-127960	Denial of service through folded HTTP response headers	8.2–8.5
CVE-2026-15353	SOAP information disclosure through malformed array dimensions	8.2–8.5
CVE-2026-129506	SOAP use-after-free when processing DTD entity references	8.2–8.5
CVE-2026-129481	Use-after-free after interrupted session shutdown	8.3–8.5
CVE-2026-129501	Double free during DOM XML serialization	8.4–8.5
CVE-2026-129182	Use-after-free via repopulation of the last fatal error backtrace after shutdown	8.5
CVE-2026-129438	Incorrect RFC 3986 URI serialization for oversized input	8.5
CVE-2026-48841	Vulnerability in uriparser used by the URI extension (updated to uriparser 1.0.3)	8.5

Source: php.net ChangeLog (19 November 2026). SHANNON LIMITED LIABILITY COMPANY https://shannon.co.jp/en/insights/php-vulnerability-checklist/