BYTEVANCER - SECURITY CHECKLIST

# PHP + Node.js Security Patch Checklist

**As of 26 Oct 2026.** Versions, stopgaps and end-of-life lines from the vendors' own advisories. Check for newer releases before you act.

Companion to the three-part series: Part 1: PHP - Part 2: Node.js - Part 3: SEO impact.

## 1. PHP: CVE-2026-109618 and CVE-2026-109619 (21 Oct 2026)

Both rated Critical, CVSS v4.0 9.2. CVE-2026-109618 (RCE via OOM corruption): "unauthenticated remote code execution as the web worker account". CVE-2026-109619 (RCE via stale global state): "unauthenticated heap use-after-free, memory disclosure and remote code execution". Affects "all PHP installations serving web requests, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed"; highest risk mod_php.

| Branch | Fixed in | Support status (php.net) |
|---|---|---|
| 8.5 | 8.5.12 | Active to 31 Dec 2027, security to 31 Dec 2029 |
| 8.4 | 8.4.27 | Active to 31 Dec 2026, security to 31 Dec 2028 |
| 8.3 | 8.3.36 | Security fixes until 31 Dec 2027 |
| 8.2 | 8.2.35 | Security-only until 31 Dec 2026 |
| 8.1, 8.0, 7.4 | No release; minimal source backports only | End of life: no updates from the PHP project |

**Partial mitigations only** ("There are no complete mitigations, updating is the only safe choice"):

- CVE-2026-109618: memory_limit=-1, a low post_max_size, or cgroup memory limits. RLIMIT_AS / RLIMIT_DATA do not help.
- CVE-2026-109619: session.upload_progress.enabled=0; fatal_error_backtraces=0 (8.5); pm.max_requests=1.
- Follow-up CVE-2026-115560 (23 Oct): session upload progress when session.serialize_handler is switched to php at runtime via ini_set(). No fixed release yet; mitigate with session.upload_progress.enabled=0.

**Exploitation status:** proof of concept public since 22 Oct (Sophos, which reports "no evidence of a successful compromise"). Not in CISA's KEV catalog as of version 2026.10.23. Older PHP bugs that are KEV-listed include CVE-2024-4577 (PHP-CGI on Windows, fixed 8.1.29 / 8.2.20 / 8.3.8) and CVE-2019-11043 (PHP-FPM).

**Earlier 2026 releases:** 24 Sep (8.2.34 / 8.3.35 / 8.4.26 / 8.5.11) and 30 Jul (8.2.33 / 8.3.33 / 8.4.24 / 8.5.9).

## 2. Node.js: October 2026 security release

10 CVEs: 4 high, 3 medium, 3 low. Headline CVE-2026-111497, a Brotli decoder out-of-bounds write: crash, process-memory leak or remote code execution when an app decompresses attacker Brotli data via node:zlib.

| Line | Fixed in (Oct 2026) | Status |
|---|---|---|
| v26 | v26.12.1 | LTS from 28 Oct 2026 to 30 Apr 2029 |
| v24 | v24.22.1 | Maintenance from 20 Oct 2026 to 30 Apr 2028 |
| v22 | v22.23.4 | Maintenance until 30 Apr 2027 |
| v25 | No fix | End of life 1 Jun 2026 |
| v20 | No fix | End of life 30 Apr 2026 (last release v20.20.2) |
| v18 | No fix | End of life 30 Apr 2025 |

Node.js: "End-of-Life versions are always affected when a security release occurs." Earlier 2026 releases: July (v22.23.2 / v24.18.1 / v26.5.1) and June (22.23.0 / 24.17.0 / 26.3.1). Some October CVEs are incomplete fixes of earlier ones, so patching is continuous.

## 3. If you don't patch

**On the server** (vendor-stated impacts):

- PHP: unauthenticated remote code execution as the web worker account; memory disclosure. On mod_php the attack can trigger "before any application code runs".
- Node.js: crash, memory leak or RCE (Brotli); DNS and TLS hostname check bypasses; predictable randomUUID() values in snapshots/SEA; July's HTTP/2 memory exhaustion DoS (v22/v24).

**In Google Search** (Google's wording):

- "This site may be hacked" shows "when we believe a hacker might have changed some of the existing pages on the site" and is removed "after we check that your site is fixed".
- Security Issues: "a warning label in search results" and "an interstitial warning page in the browser". Premature review requests can get you "marked as a repeat offender".
- "Sites that violate our policies may rank lower in results or not appear in results at all."
- "5xx and 429 server errors prompt Google's crawlers to temporarily slow down with crawling"; URLs that persistently return server errors are eventually dropped from the index.

## 4. Patch-day checklist

1. Inventory every runtime: servers, containers, CI images. Run `php -v`, `php -i | grep -i "Server API"` and `node -v`.
2. Priority 1: PHP serving web requests below 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12. Patch today; apply the stopgaps above only if you can't patch within hours.
3. Priority 2: PHP 8.1 or older, or Node.js v18 / v20 / v25. Upgrade the line; there is no official fix.
4. Priority 3: Node.js below v22.23.4 / v24.22.1 / v26.12.1.
5. Back up, patch on staging, run your tests, then patch production.
6. Restart PHP-FPM, Apache or the Node processes, then re-run the version checks.
7. Check Search Console's Security Issues report and watch for server errors.
8. If anything was flagged: clean every page, then request review once.

## Sources


https://www.php.net/archive/2026.php#2026-10-21-5

https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp

https://www.php.net/archive/2026.php#2026-10-23-1

https://www.php.net/supported-versions.php

https://github.com/php/php-src/security/advisories/GHSA-3qgc-jrrr-25jv

https://www.sophos.com/blog/proof-of-concept-exploit-released-for-php-vulnerabilities-109618-109619

https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

https://nodejs.org/en/blog/vulnerability/july-2026-security-releases

https://nodejs.org/en/blog/vulnerability/june-2026-security-releases

https://github.com/nodejs/release#release-schedule

https://support.google.com/websearch/answer/190597

https://support.google.com/webmasters/answer/9044101?hl=en

https://developers.google.com/search/docs/essentials/spam-policies#hacked-content

https://developers.google.com/crawling/docs/troubleshooting/http-status-codes


Want this handled for you? ByteVancer website maintenance and security patching. Full write-up: the PHP and Node.js security series.