PHP2SHELL RESPONSE CHECKLIST · CVE-2026-109618 · CVE-2026-109619

# From emergency patch to audit-ready in 90 days

Fixed versions: **8.5.12 · 8.4.27 · 8.3.36 · 8.2.35**. Updating WordPress or your application does not update PHP. Restart every PHP worker after patching.

## 1 Triage — FIRST 24 HOURS

- [ ] Inventory every PHP runtime and its exact version
- [ ] Flag internet-facing, mod_php, and ARM64 systems as priority one
- [ ] Assign an owner to every system
- [ ] Open an emergency change or incident record

**Evidence:** Asset list with versions and owners **Owner:** _____ **Done:** __/__

Asset inventory · Vulnerability ID

## 2 Contain & patch — DAYS 1 TO 3

- [ ] Patch to 8.5.12, 8.4.27, 8.3.36, or 8.2.35
- [ ] Restart Apache, PHP-FPM, and every PHP worker
- [ ] Apply interim mitigations where patching must wait
- [ ] Get written patch confirmation from hosts and vendors

**Evidence:** Change tickets, vendor confirmations, exception requests **Owner:** _____ **Done:** __/__

Patching · Change & config · Third parties

## 3 Verify & hunt — WEEKS 1 TO 2

- [ ] Rescan to confirm fixed versions are running
- [ ] Review logs for memory-limit errors, HTTP 500 bursts, oversized PHPSESSID cookies, and worker crashes
- [ ] Escalate anything suspicious to incident response

**Evidence:** Scan results and a hunt report **Owner:** _____ **Done:** __/__

Vulnerability ID · Detection & IR

## 4 Document & close — BY DAY 30

- [ ] Update the risk register: owner, status, residual risk
- [ ] Approve exceptions with deadlines and compensating controls
- [ ] Brief leadership on exposure, actions, and open items

**Evidence:** Risk register entries, approved exceptions, leadership summary **Owner:** _____ **Done:** __/__

Risk register

## 5 Strengthen — BY DAY 90

- [ ] Plan upgrades off PHP 8.2 before its December 31, 2026 end of support
- [ ] Add language runtimes to lifecycle tracking
- [ ] Add patch-notice and SLA clauses to hosting and vendor contracts
- [ ] Set and measure remediation targets for critical, internet-facing flaws

**Evidence:** End-of-life plan, updated standards and contracts, metrics **Owner:** _____ **Done:** __/__

End-of-life · Third parties · Patching

CONTROLS CROSSWALK

# One response. Five frameworks. The same evidence.

Colored markers match the tags on page 1, so each checklist item traces to the controls it satisfies.

| Control area | NIST CSF 2.0 / 800-53 | ISO/IEC 27001:2022 | CSA CCM v4.0 | FFIEC IT Handbook | SOX (ITGCs) |
|---|---|---|---|---|---|
| **Asset inventory** | ID.AM-01, ID.AM-02 / CM-8 | A.5.9 | DCS-06 | InfoSec II.C.5 | In-scope system scoping |
| **Vulnerability identification & threat intel** | ID.RA-01, ID.RA-02, ID.RA-08 / RA-5, SI-5 | A.8.8, A.5.7 | TVM-05, TVM-07, TVM-08 | InfoSec III.A; AIO VI.B.3 | IT ops monitoring |
| **Patching (flaw remediation)** | PR.PS-02 / SI-2 | A.8.8 | TVM-03 | InfoSec II.C.10(d); AIO VI.B.3 | Change mgmt |
| **Change & configuration** | PR.PS-01 / CM-3, CM-6 | A.8.9, A.8.32 | CCC-01, CCC-06 | InfoSec II.C.10(a) | Change mgmt |
| **End-of-life software** | ID.AM-08 / SA-22 | A.5.9, A.8.8 | TVM-05, DCS-06 | InfoSec II.C.11 | IT ops; change mgmt |
| **Risk register & treatment** | ID.RA-05, ID.RA-06 / RA-3 | Cl. 6.1.2, 6.1.3, 8.2, 8.3 | GRC-02 | InfoSec II.A | COSO Principles 7 and 11 |
| **Detection & incident response** | DE.CM-09, DE.AE-02, RS.MA-01 / SI-4, IR-4 | A.8.16, A.5.24, A.5.25, A.5.26 | LOG-03, LOG-05, SEF-03, SEF-06 | InfoSec III.B, III.C, III.D | IT ops: incident mgmt |
| **Third-party & hosting providers** | GV.SC-07 / SA-9, SR-6 | A.5.19, A.5.21, A.5.22 | STA-08, STA-12 | InfoSec II.C.14, II.C.20 | SOC 1 reports & CUECs |

SOX does not prescribe patching directly; it reaches it through IT general controls over systems that support financial reporting. Control IDs use NIST CSF 2.0, NIST SP 800-53 Rev. 5, ISO/IEC 27001:2022, CSA Cloud Controls Matrix v4.0 (v4.1 released January 2026 adds 11 controls), and the FFIEC IT Examination Handbook. Verify mappings against the versions you're assessed on.

**Official sources:** NIST CSF 2.0: doi.org/10.6028/NIST.CSWP.29 · NIST SP 800-53 Rev. 5: csrc.nist.gov · ISO/IEC 27001:2022: iso.org/standard/27001 (paid) · CSA CCM: cloudsecurityalliance.org/research/cloud-controls-matrix · FFIEC: ithandbook.ffiec.gov · SOX: govinfo.gov (Public Law 107-204) · PCAOB AS 2201: pcaobus.org · COSO: coso.org
**Vulnerability details:** thephp.foundation (October 21, 2026 security release)

## Exceptions and open items

| System / owner | Reason it can't be patched yet | Compensating control | Target date | Approved by |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |