CONTINUITY HUB

Precautionary Outage Quick Card: Unpatchable PHP & Critical Vulnerability Protocol

OPERATIONAL CONTINUITY REFERENCE • POST 653
Current version — Nov 1, 2026. Update history: https://continuityhub.org/how-should-an-organization-plan-a-precautionary-outage-when-a-critical-vulnerability-cannot-be-patched-at-once/

THE PRECAUTIONARY OUTAGE REALITY: ACT BEFORE EXPLOIT CONFIRMATION

On **October 21, 2026**, PHP released emergency fixes for two critical unauthenticated remote code execution vulnerabilities: **CVE-2026-109618** and **CVE-2026-109619** (rated **CVSS v4.0 9.2**). Insurer **Coalition** detected in-the-wild exploit attempts >5 hours before official patch release. Scope encompasses **all web-serving PHP** (PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, LiteSpeed). **CISA's operational directive**: organizations that cannot update immediately, or running unsupported **PHP 8.1 or earlier**, must take systems offline until patched.

1. INVENTORY BEFORE DECIDING ANYTHING

Standing Artifact

You cannot sequence an outage for systems you have not found.

- **Hidden Prevalence Warning (CISA):** PHP is frequently bundled inside third-party software and not directly visible as a standalone service.
- **Admin Tools First (Coalition):** Actively scan for PHP running administrative tools managing firewalls, databases, phone systems (PBX), and backups.
- **Full Scope Audit:** Catalog public websites, internal staff tools, vendor appliances, and control panels (cPanel, Plesk).
- **Standing Plan Requirement:** Maintain a standing asset register refreshed before emergencies, recording a named owner and verified patch route for every copy.
- **End-of-Life (EOL) Flag:** PHP 8.1 and older receive zero project patches. Coalition rule: upgrade immediately, obtain vendor backport, or take off the internet.

2. SET DECISION RULE BEFORE THE EMERGENCY

Everbridge Framework

Write the threshold in calm conditions — not during night-shift stress.

- **Important Business Services:** Define which business services must be protected vs those that can tolerate planned shutdown.
- **Impact Tolerances:** Specify the exact maximum allowable disruption (hours/days) each service can sustain before unacceptable operational harm.
- **State Preference Hierarchy:**
  1. *Patch in place* (if patch deploys & tests within tolerance window)
  2. *Isolate from internet* (restrict access to VPN/internal IPs)
  3. *Take fully offline* (graceful server/service shutdown)
- **CISA Default Rule:** Patch internet-facing systems immediately; if a system cannot be updated at once, take it offline until it can be.
- **Actionable Night-Shift Threshold:** "*We will take the service offline if a fixed version cannot be deployed and verified within the window our impact tolerance allows.*"

PRECAUTIONARY TRIAGE & EXPOSURE MATRIX

Operational Guide

System Type / Tier	PHP Environment & Scope	Default Action Rule	Verification & Fallback
Admin Tools Firewalls, DBs, Backups, PBX	PHP-FPM, Apache, vendor bundled. Holds cross-system master credentials.	**Remediate First (Coalition)**	Isolate from internet immediately; patch or take offline within 2 hours.
Internet-Facing Web Public portals, e-commerce, APIs	PHP 8.2 – 8.5 active versions. Exposed to unauthenticated RCE.	Prioritize Patching (CISA)	Deploy 8.5.12, 8.4.27, 8.3.36, or 8.2.35+; restart workers; offline if window exceeds tolerance.
EOL PHP Deployments **PHP 8.1, 8.0, 7.x, 5.x**	Unsupported legacy stacks, vendor appliances, unmaintained cPanel/Plesk.	**Take Off Internet**	Zero project patches exist. Upgrade stack, secure vendor backport, or remain permanently offline.
Internal Staff Tools Intranets, ERPs, billing tools	Internal network only, no public IP. Secondary pivot target.	Isolate & Bridge	Apply interim hardening bridge settings; schedule staged patch within 24 hours.

3. SEQUENCE THE OUTAGE, DON'T JUST ANNOUNCE

Execution Standard

- **Exposure-Driven Sequence:** Remediate internet-facing systems first (CISA) and administrative control tools first (Coalition).
- **Target Secure Versions:** Update to PHP **8.5.12**, **8.4.27**, **8.3.36**, or **8.2.35** or later.
- **Mandatory Worker Restart:** Patching is not finished upon file install. You must restart `php-fpm`, Apache, or web server workers to flush memory.
- **Vendor Version Parity:** Distribution packages (Debian, RHEL, Ubuntu) or hosting bundles often use custom revision strings; confirm backport fixes directly with vendor.
- **Valtori Restoration Lesson (Reuters):** Finland's state IT provider Valtori planned days-to-weeks restoration because systems require careful testing alongside updates. Budget for verification, not just installation.

BOUNDED & EXPIRING BRIDGE MEASURES

Partial Hardening

PHP & CISA warning: Bridge measures DO NOT make an installation safe.

- `session.upload_progress.enabled=0` in php.ini with a full restart of every PHP worker process.
- `memory_limit` strictly locked so application code cannot override it.
- `post_max_size` reduced to minimal necessary threshold.
- **WAF Virtual Patching:** Deploy Web Application Firewall rules to block raw multipart exploit probes.
- **Dated Expiring State:** Log what was applied, applied timestamp, residual risk, and a hard deadline by which the service is patched or taken offline.

4. PRE-APPROVED HOLDING STATEMENTS

HUB International Model

Pre-vetted holding statements prevent panic and document voluntary defense:

1. **What:** Exactly which services are taken offline.
2. **Why:** Oct 21 critical vulnerability (CVE-2026-109618/19, CVSS 9.2).
3. **Action:** Vendor patch deployment & staging verification underway.
4. **Cadence:** Specific time for the next status update.

Preserve all employee and customer communication logs — required for insurance claims (Crestview Public Adjusters).

5. FORENSIC COMPROMISE DIAGNOSTIC

Coalition & CISA Indicators

Document "*We looked, and here is what we found*" with timestamps:

- **Shell & Tool Spawns:** PHP workers launching `/bin/sh`, `cmd.exe`, `curl`, or `wget`.
- **Web Root Integrity:** New or altered files in docroot or upload directories.
- **Persistence:** Unauthorized cron jobs, scheduled tasks, or new local user accounts.
- **Upload & Crash Patterns:** Upload spikes followed by Out-of-Memory (OOM) or bursts of HTTP 500 errors.
- **Worker Stability:** Repeatedly crashing or segfaulting PHP-FPM worker pools.

6. INSURER-GRADE CLAIMS PACKET (BEAZLEY & CRESTVIEW EVIDENCE AUDIT)

Claims Compliance

Beazley Forensic Accountant Requirements:
• Daily operational & transaction records (loss period vs. prior year)
• Monthly billings and collections over at least 12–24 months
• Prior year federal/state tax returns & monthly P&L statements
• Weekly payroll logs for outage window & prior year
• Service scheduling logs showing cancellations & make-up hours

Crestview Technical Claim Documentation:
• System event logs & forensic reports establishing timeline
• IT downtime duration reports & uptime monitoring records
• Customer communication logs where deliveries/services were affected
• Itemized invoices for extra restoration expenses & contractor overtime
• Prompt notice record to cyber broker and insurance carrier