



Guidance to the State of Idaho on Mitigating PHP2Shell Vulnerabilities

Action Checklist

- Inventory all PHP systems.
- Patch immediately recommended PHP versions.
- Remove unpatchable systems from public access.
- Enable temporary WAF protections as needed.
- Enable enhanced logging and monitoring.
- Follow established reporting processes
- Replace unsupported PHP systems.

Purpose

This document presents **guidance** to the State of Idaho, based primarily on **U.S. Federal cybersecurity direction** (CISA, NSA, FBI). It provides actionable steps for Idaho agencies, local governments, public schools, tribal entities, and critical infrastructure operators responding to the PHP2Shell vulnerabilities (CVE-2026-109618 & CVE-2026-109619).

1. Federal Resources

Cybersecurity and Infrastructure Security Agency (CISA)

CISA recommends that organizations:

- Patch immediately to **PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35**.
- Inventory all PHP-based systems, including embedded or vendor-managed platforms.
- Prioritize patching of internet-facing and public-facing services.

- Take systems offline if they cannot be patched immediately.
- Use WAFs only as temporary protection.
- Monitor for suspicious PHP activity, such as processes launching shells or downloading files.

National Security Agency (NSA)

NSA emphasizes:

- Rapid statewide inventory of all systems that depend on PHP.
- Quick deployment of vendor patches across all environments.
- Enhancing logging to improve detection and response.
- Phasing out end-of-life PHP versions.
- Removing unpatchable systems from service until mitigated.

Federal Bureau of Investigation (FBI)

FBI guidance for organizations includes:

- Identifying and prioritizing vulnerable PHP systems.
- Monitoring for compromise indicators such as shell execution or unexpected downloads.
- Isolating affected systems and preserving logs.
- Reporting incidents to **IC3.gov** or the nearest FBI field office.
- Taking unpatchable systems offline until secure.

2. Recommended Actions for Idaho

Step 1: Perform a PHP Inventory

- Identify where PHP exists.
- Include websites, internal applications, cloud services, vendor systems, and appliances.
- Confirm PHP versions and patch timelines with vendors.
- Patching should not wait until the vulnerability list is complete. Additional scanning should be done to confirm the patching is successful.

Step 2: Enforce Immediate Patching Across Idaho

- All systems should be updated to the approved PHP versions.
- Public-facing services should not remain online until patched.
- Any system that cannot be updated in a timely manner should be temporarily removed from public access.

Step 3: Apply Interim Protections When Patching Is Not Immediate

- Use WAF-based protections as a short-term buffer.
- Enable enhanced logging per NSA recommendations.
- Increase monitoring for abnormal behaviors, especially PHP launching unexpected processes.

Step 4: Strengthen Monitoring and Incident Response

- Instruct cybersecurity teams to watch for:
 - PHP processes launching shells
 - Unauthorized downloads
 - Memory exhaustion issues
- Follow established reporting processes
- Isolate and preserve logs for any system showing suspicious activity.

Step 5: Modernize PHP Infrastructure

- Replace outdated PHP systems.
- Enforce recurring PHP patch cycles.
- Conduct audits to confirm PHP compliance.
- Retire or upgrade systems that can no longer receive security patches.