Archdiocese of Seattle

October 26, 2026

TECHNICAL SECURITY ADVISORY

TO: Parish Administrators, School IT Leads, Directors of Technology, and Systems Engineers

FROM: Office of Information Security / IT Services – Archdiocese of Seattle

DATE: October 22, 2026

SUBJECT: CRITICAL ACTION REQUIRED: Core PHP Remote Code Execution Vulnerabilities (CVE-2026-109618 & CVE-2026-109619)

SEVERITY: CRITICAL (CVSSv4 Score: 9.2)

TARGET AUDIENCE: All staff managing web servers, hosted CMS platforms (WordPress, Drupal), local network gear, and IoT equipment across Archdiocesan parishes, schools, and central agencies.

Executive Summary

A pair of critical, unauthenticated Remote Code Execution (RCE) vulnerabilities—dubbed **"PHP2Shell"**—have been publicly disclosed in core PHP engine components:

- **CVE-2026-109618:** Out-of-memory (OOM) handling memory corruption during request initialization.
- **CVE-2026-109619:** Use-after-free (UAF) execution via stale request-owned global state.

These flaws allow unauthenticated attackers to execute arbitrary code on vulnerable systems via crafted HTTP web requests. **Because PHP is embedded inside many non-traditional network technologies, this alert applies to web hosting, network infrastructure, and administrative devices.**

Scope of Risk: Not Just Websites

While standard web applications (WordPress, Drupal, custom parish portals) are primary targets, **dedicated equipment across parish and school networks frequently runs PHP under the hood** to power administrative web consoles and management dashboards.

High-Risk Asset Inventory Across Parishes & Schools:

1. **Public Web Servers:** Parish websites, school portals, and donation forms hosted on dedicated or virtual web servers (Apache mod_php, PHP-FPM, LiteSpeed, or Nginx backends).
2. **Network Infrastructure Consoles:**
    - **Firewalls & Routers:** Embedded web GUIs on edge firewalls (e.g., pfSense, OPNSense, legacy Fortinet/SonicWall models).
    - **Managed Switches & Wireless Controllers:** Local management consoles for Wi-Fi access points and managed network switches.
    - **Network-Attached Storage (NAS):** Storage appliances (e.g., Synology, QNAP, TrueNAS) running PHP-based web admin panels.
3. **Smart Campus & Facilities Devices:**
    - **IP Security Camera Systems (NVRs/DVRs):** Web viewers and camera management portals.
    - **HVAC / Access Control Panels:** Smart building controllers and electronic door access management interfaces exposed to internal or external networks.

Affected Versions

- **Vulnerable:** All versions of PHP from **5.4 through 8.5.11**.
- **Fixed Runtimes:** Upgraded to PHP **8.5.12**, **8.4.27**, **8.3.36**, or **8.2.35**.
- **Unsupported Runtimes:** PHP 8.1 and earlier are End-of-Life (EOL) and **will not receive vendor patches**. Devices running legacy PHP runtimes must be isolated or updated via vendor firmware releases.

Required Technical Action Items

Please execute the following remediation steps immediately within your respective locations:

Step 1: Inventory & Scan Non-Standard Equipment

- Audit all networked hardware in your school or parish with a web management console.
- Check vendor support portals (e.g., Synology, pfSense, camera vendors, switch manufacturers) for emergency firmware updates issued after October 20, 2026 addressing these PHP CVEs.

Step 2: Immediate Web Server Patching

- **Linux/Hosted Servers:** Upgrade PHP packages via system package managers or pull updated container base images.
- **WordPress / CMS Hosting:** Ensure server environments managed by third-party hosting vendors (WP Engine, GoDaddy, Bluehost, AWS) have updated the underlying PHP runtime to a patched version.

Step 3: Enforce Network Access Control (Mitigation)

- **Disable Remote Management Consoles:** Never expose device management panels (firewalls, NAS, access control, NVRs) directly to the public internet.
- **Isolate on Management VLANs:** Move all IoT, access control, and network device management interfaces to an isolated Administrative VLAN accessible only via secure local access or an encrypted VPN.
- **Restrict Access:** Restrict HTTP/HTTPS management ports (80, 443, 8080, 8443) on internal appliances to trusted management IP subnets.