Archdiocese of Seattle

October 26, 2026

SECURITY ADVISORY

TO: Pastors, Principals, Parish Business Managers, Administrative Staff
FROM: Office of Information Security & IT Services, Archdiocese of Seattle
DATE: October 22, 2026
SUBJECT: Urgent Security Updates Required for Websites and Internet-Connected Systems
ACTION REQUIRED: Please review and forward to your technology provider by the next business day.

Currently, there are serious PHP security vulnerabilities affecting technology systems**.**
If affected systems are not updated, a cybercriminal may gain unauthorized access to websites, network equipment, security systems, or other internet-connected devices.

Cybercriminals target organizations that delay software and firmware updates. Parishes and schools rely on technology to support ministry, communications, education, administration, and stewardship. Keeping technology systems updated is one of the most effective ways to protect parishioner information and maintain reliable operations.

What Could Be Affected?

This issue affects all devices managed through a web browser, including:

Websites and Online Services

- Parish and school websites
- Online registration forms
- Online giving and payment systems
- Other web-based applications or portals

Building and Office Systems

- Security camera systems
- Door access and keycard systems
- Internet routers and firewalls
- Wi-Fi management equipment
- Network storage devices

- Smart building or HVAC control systems

What You Should Do

If You Have a Technology Provider or IT Support Partner

Connect with your IT support team immediately and ask them to:

1. **Review all websites and web-hosted services** to ensure current security updates have been applied.

2. **Check internet-connected equipment** for available firmware or security updates and install them if available.

3. **Confirm that management or administration pages are not publicly accessible from the internet.**

4. **Review older equipment** to determine whether it is still supported by the manufacturer and receives security updates.

Please send this technical document to them.

If You Manage Your Own Website

Contact your website provider or hosting company and ask:

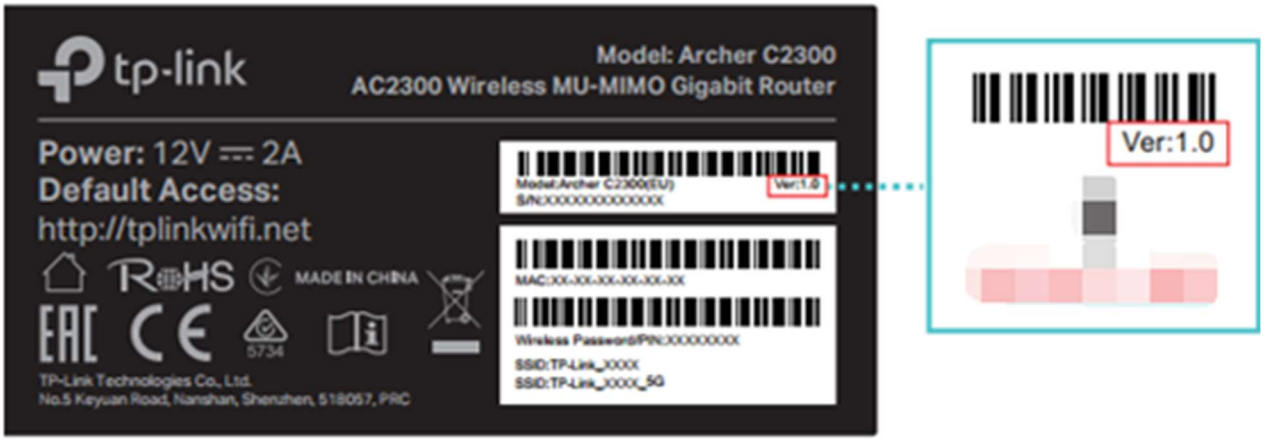
"Have all recommended security updates related to the October 2026 PHP vulnerabilities been applied to our website and hosting environment?"

Older equipment alert

Some older network devices, security systems, and building management equipment may no longer receive security updates from their manufacturers. In these cases, additional protective measures may be required to reduce risk. Your technology provider can help determine whether any equipment needs to be upgraded, isolated, or replaced.

Here is how to check your router's end-of-life information:

- https://www.router-switch.com/eol-eosl-checker/
- https://www.asus.com/ca-en/support/faq/1047671/
- https://www.tp-link.com/us/suport/faq/3562/



Checking Network & Smart Devices (Routers, Switches, IoT)

- Web Admin Portal: Access the device's IP address via browser (e.g., 192.168.1.1), log in, and check the System, Status, or About page.
- Mobile Management Apps: Open the dedicated management app (e.g., TP-Link Tapo, Google Home), navigate to Device Settings, and check Hardware/Firmware Info.
- Command Line (Managed Switches/Enterprise): Connect via SSH/Console and execute commands like show version (Cisco/Aruba) or display version (Huawei).

Best Practices

- Always backup: Create system restore points or back-up device configurations before applying BIOS or firmware updates.
- Verify Hardware revisions: Never install firmware built for a different hardware version (e.g., updating a v2 device with v1 firmware can brick the hardware).