नेपाल सरकार

प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय

सूचना प्रविधि तथा विद्युतीय शासन कार्यालय

राष्ट्रिय साइबर सुरक्षा केन्द्र

सिंहदरबार, काठमाडौं

प.स.:२०८३/०८४

च.नं.:

मिति:२०८३/०७/०५ गते बिहीबार

अत्यन्त जरुरी साइबर सुरक्षा एडभाइजरी

हालै PHP र सोसँग सम्बन्धित Runtime (Apache mod_php, PHP-FPM, php-cgi, FrankenPHP, LiteSpeed आदि) तथा Ecosystem (WordPress, Joomla, Drupal, Magento आदि) मा देखिएको दुई गम्भीर Vulnerability (CVE-2026-109618 र CVE-2026-109619) का सम्बन्धमा तत्काल निम्न व्यवस्था गर्न सम्बन्धित सबैमा यो सुरक्षा एडभाइजरी जारी गरिएको छ ।

१. सम्बन्धित निकायको प्रणालीमा प्रयोग भएको PHP लाई यथाशीघ्र तपसिलको प्रक्रिया अवलम्बन गरी **८.५.१२ +, ८.४.२७+, ८.३.३६+ वा ८.२.३५+** मा अपग्रेड गर्नुहोस् ।

२. **८.१ वा पुरानो Version** का लागि Fix/Patch नआएकोले यस्ता वेबसाइटलाई अनिवार्य रुपमा नयाँ सुरक्षित संस्करण (Latest Secured Version) मा लैजानुहोस्।

३. Patch Deployment का सम्बन्धमा थप प्राविधिक सहजीकरणका लागि यस केन्द्रका कम्प्युटर अधिकृत श्री आशिष भट्ट (सम्पर्क: 9844682742) र प्रणाली पहुँचमा सहजीकरणका लागि एकीकृत डाटा व्यवस्थापन केन्द्र (IDMC) मा सम्पर्क गर्नुहुन अनुरोध छ ।

तपसिल:

Step 1: How to Identify

1. Check your running PHP version
   php -v
2. If you run web services (PHP-FPM/Apache), verify the active server version (*php-fpm -v)*
3. For Debian/Ubuntu (*dpkg -l 'php*' | grep '^ii'*) and RHEL/Fedora-Family systems (*rpm -qa | grep -E '^php'*)
4. Use any of the following applicable scripts to inspect and identify the issue and version before and after the fix

https://github.com/NCSC-NL/php2shell
https://github.com/0xrsydn/php2shell-scan (A lightweight Python Utility)
https://github.com/nukIeer/CVE-2026-109618-109619-checker
https://github.com/sxyrxyy/php2shell-cve-2026-109618-check
https://github.com/corelight/php2shell-detect (Detection rules)

Step 2: How to Patch & Fix

Upgrade your environment to the official patched versions immediately:

- **PHP 8.5:** Upgrade to **8.5.12 or later**
- **PHP 8.4:** Upgrade to **8.4.27 or later**
- **PHP 8.3:** Upgrade to **8.3.36 or later**
- **PHP 8.2:** Upgrade to **8.2.35 or later**

System Commands for upgrade:

- **Ubuntu/Debian:** *sudo apt update &&sudo apt upgrade php*
- **RHEL/Rocky/CentOS:** *sudodnf update php*
- **Docker Users:** Update your base images (e.g., php:8.3-fpm-alpine) and rebuild container images.

Restart everything.
Patching the binary on disk does nothing for running processes. **Restart PHP-FPM, Apache, and every long-running PHP worker** (queue workers, schedulers, daemons) so the patched binary is loaded.

Validate

Review the official advisories for both vulnerabilities and confirm whether your exact PHP build contains the fixes.
https://www.php.net/archive/2026.php
CVE-2026-109618:
https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
CVE-2026-109619:
https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp

Step 3: Full-Service Isolation (If Patching or Mitigations Must Wait)

When to Use: Prioritise internet-facing systems. If a verified fix cannot be applied promptly, restrict public access or isolate the affected service. WAF and firewall rules may provide additional risk reduction, but the PHP project states that there are no complete mitigations: updating is the only safe choice.

- Restrict Network Access: Take exposed PHP applications off the public web. Enforce access strictly through an internal VPN, explicit IP allowlist, or Zero-Trust gateway
- Isolate EOL & High-Risk Stacks: If you run end-of-life PHP versions (8.1 or older) that receive no upstream security releases, place them into isolated network sandboxes and block egress traffic to stop lateral movement.
- Stop Vulnerable Services: If an internet-facing service cannot be patched or shielded, temporarily halt the runtime processing daemon:

  - **PHP-FPM:** *sudosystemctl stop php*-fpm*
  - **Apache:** *sudosystemctl stop apache2 (or httpd)*
  Windows: Stop the respective Windows Services via services.msc or PowerShell (*Stop-Service w3svc, Stop-Service apache2.4*).
  - **Docker / Cloud Run:** Scale deployments down to 0 replicas (*docker stop <container> or kubectl scale deployment <app> --replicas=0)*.