



National Cyber Emergency Response Team

Government of Pakistan



NCA-19.211026 – National CERT Advisory

Critical PHP Vulnerabilities (CVE-2026-109618 and CVE-2026-109619): Potential Unauthenticated Remote Code Execution

National CERT Pakistan has been monitoring reports of two critical vulnerabilities in the PHP runtime, each assigned a CVSS v4.0 score of 9.2/10, that may allow unauthenticated remote code execution (RCE) on internet-facing PHP systems. The PHP Security Team has confirmed the two vulnerabilities and has released the fix and asks all users to update immediately. Publicly circulating exploit demonstrations (reported as “PHP2Shell”) and early attack activity have also been reported.

This advisory recommends organizations to prepare for emergency patching, reduce exposure, apply compensating controls, and strengthen monitoring.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-19.211026
Threat Type	Remote Code Execution (Potentially Unauthenticated) in the PHP Runtime
Severity	Critical (CVSS v4.0 Base Score 9.2/10 for each vulnerability)
Attack Vector	Malicious HTTP requests to internet-facing PHP applications; reported leads include multipart/form-data request processing and session upload-progress handling (unconfirmed)
Authentication Required	None reported (potentially unauthenticated; pending vendor confirmation)
User Interaction	None Required
Risk Rating	Critical (Confidentiality, Integrity & Availability Impact)
Scope & Applicability	Federal & Provincial Government portals, Critical Information Infrastructure (CII), Financial Institutions, E-Commerce Platforms, Web Hosting Providers, and all organizations operating PHP-based public-facing services

IMPACT ANALYSIS

Successful exploitation of these vulnerabilities may plausibly result in:

1. **Remote Code Execution:** Arbitrary command execution on the underlying web server.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



2. **Unauthorized Server Access:** Initial foothold on hosting infrastructure for follow-on attacks.
3. **Malware and Web-Shell Deployment:** Persistent malicious access to compromised servers.
4. **Credential Theft:** Exposure of application, database, and API credentials stored on the server.
5. **Data Exfiltration:** Theft of citizen, customer, or organizational data held by PHP applications.
6. **Website Defacement:** Public tampering with government, commercial, and e-commerce web content.
7. **Service Disruption:** Outage of portals, web applications, and online services.
8. **Compromise of CMS and Commerce Platforms:** Exposure of WordPress, Joomla, Drupal, Magento, and similar platforms running on a vulnerable PHP runtime.

The precise privileges obtained and the resulting impact depend on server configuration and the final vulnerability details.

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Critical Remote Code Execution Vulnerabilities in a Server-Side Language Runtime
Threat Status	Active – Exploit demonstrations and early malicious activity reported; vendor patches pending
Target Scope	Government, CII, Financial Sector, E-Commerce, Hosting Providers, Private Enterprises
Attack Complexity	Not yet confirmed; at least one vulnerability (reportedly CVE-2026-109618) has been reproduced by researchers
Privileges Required	None reported (provisional)
Affected Systems	PHP runtime itself; exposure possibly extends to PHP 5 onward (some researchers report PHP 5.4 and later). Affected-version matrix to be confirmed by PHP
Reference Classifications	CVE-2026-109618 (CVSS v4.0: 9.2), CVE-2026-109619 (CVSS v4.0: 9.2); “PHP2Shell” exploit chain (reported)

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should actively monitor for:

1. Internet-facing PHP applications running on unpatched or unsupported PHP versions.

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



2. End-of-life PHP 8.1 or older runtimes in production, for which no official upstream fix is expected.
3. Unusual or high-volume multipart/form-data POST requests, particularly to endpoints that do not normally accept uploads.
4. Requests targeting PHP session upload-progress functionality.
5. Newly created or recently modified .php files in web roots and upload directories (possible web shells).
6. Web-server or PHP-FPM worker processes spawning shells or unexpected child processes.
7. Unexpected outbound connections from web servers.
8. WAF, EDR, or web-server alerts referencing PHP exploitation attempts or "PHP2Shell" activity.
9. Unexplained changes to configuration files, scheduled tasks, or user accounts on PHP hosts.
10. Hosting providers, containers, or managed services with no confirmed PHP patch timeline.

REMEDIATION ACTIONS

1. Priority Remediation and Mitigation Controls (MANDATORY)

Action Category	Specific Actions
Asset Identification	Inventory PHP versions across servers, virtual machines, containers, hosting panels, embedded applications, and managed services
Exposure Reduction	Restrict unnecessary public access; temporarily isolate critical services where adequate mitigation is unavailable
Patch Preparation	Identify deployment owners, obtain approvals, back up applications and configurations, and prepare a rollback plan
Patch Deployment	On official release, deploy verified fixes to supported PHP branches via trusted vendor channels, prioritizing internet-facing and high-value systems
Compensating Protections	Enable applicable WAF protections and restrict unnecessary upload endpoints, without assuming complete protection
Threat Monitoring	Inspect web-server, WAF, PHP-FPM, system, and EDR telemetry for abnormal requests or server activity
Unsupported Versions	Migrate end-of-life PHP deployments or isolate them until a supported, patched runtime is available

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



Action Category	Specific Actions
Remediation Validation	Verify the actual loaded runtime, package build, and effective security fix; conduct application smoke tests

2. Emergency Patch Status – Supported PHP Branches

The latest stable releases published on the official PHP website at the time of verification, and the emergency versions reportedly expected, are:

PHP Branch	Latest Published Release Found	Emergency Patch Reportedly Expected
PHP 8.5	8.5.11	8.5.12
PHP 8.4	8.4.26	8.4.27
PHP 8.3	8.3.35	8.3.36
PHP 8.2	8.2.34	8.2.35
PHP 8.1 and older	End-of-life upstream	No official upstream fix expected

Important Clarification: The vulnerabilities affect the PHP runtime itself. Updating WordPress, Joomla, Drupal, Magento, or their plugins does not necessarily replace or secure the underlying PHP runtime. A separate server-level or hosting-provider update is required. Once released, obtain patches from the official PHP downloads page or trusted operating-system, container-image, or hosting-provider package channels.

3. Temporary PHP Configuration Hardening (Risk Reduction Only)

Some researchers recommend the following temporary measures while awaiting definitive patches. They are not a confirmed fix for either vulnerability and must not delay patching, isolation, or other protections. Assess application compatibility before applying.

Control	Specific Actions
<code>session.upload_progress.enabled</code>	Set to Off in php.ini to disable session upload-progress tracking
<code>session.use_strict_mode</code>	Set to On in php.ini

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk

Control	Specific Actions
Multipart Request Filtering	Apply targeted WAF or web-server rules to restrict unnecessary multipart requests; a blanket block may disrupt file uploads, administration functions, and application transactions

4. Verifying PHP Deployments (Linux)

Administrators can start with the following diagnostic commands:

Check	Command	Platform
CLI PHP version	<code>php -v</code>	All Linux
PHP binary location	<code>command -v php</code>	All Linux
Loaded configuration files	<code>php --ini</code>	All Linux
Running PHP-FPM processes	<code>ps aux grep '[p]hp-fpm'</code>	All Linux
Installed PHP packages	<code>dpkg -l 'php*'</code>	Debian / Ubuntu
Installed PHP packages	<code>rpm -qa grep -i '^php'</code>	RHEL family

Verification Guidance:

1. The command-line PHP version may differ from the runtime serving websites. Verify the web-serving SAPI, PHP-FPM pools, containers, and virtual hosts before closing a remediation ticket.
2. After patching, confirm the loaded runtime, package build, and effective security fix, and run application smoke tests.
3. Retain the package version, patch evidence, deployment timestamp, asset owner, and validation results for auditability.
4. Obtain patches only from the official PHP downloads page or trusted operating-system, container-image, or hosting-provider channels.



National Cyber Emergency Response Team

Government of Pakistan



5. Reference Sources and Verification Status

Source	Information Provided	Status
PHP Security Team	Confirmation of two critical vulnerabilities (CVSS v4.0: 9.2) and the emergency release schedule	Confirmed
Australian Cyber Security Centre (ACSC)	Acknowledges media reporting of the CVE identifiers; notes technical details not yet published	Official – partial
CERT-EU	Indicates possible exposure from PHP 5 onward	Provisional
Huntress / watchTowr Researchers	Reproduction of at least one vulnerability (reportedly CVE-2026-109618); “PHP2Shell” exploit chain	Researcher report
Tenable Research	Expected emergency fix versions for supported PHP branches	Not yet validated
Cloudflare	Reported early attacks on 21 October 2026 and temporary WAF protections	Vendor report

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Asset Inventory	Identify all PHP runtimes across servers, containers, hosting panels, and managed services
Exposure Reduction	Restrict public access or isolate critical services lacking adequate mitigation
Emergency Patching	Deploy official PHP fixes immediately upon release via trusted channels
Compensating Controls	Enable WAF protections and apply temporary PHP hardening where compatible
Threat Hunting	Review web, WAF, PHP-FPM, system, and EDR logs for abnormal activity
Legacy Migration	Migrate or isolate end-of-life PHP 8.1 and older deployments
Patch Validation	Verify loaded runtime and fix; retain audit evidence

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Monitor web-server and WAF logs for anomalous multipart/form-data requests
2	Detect requests targeting PHP session upload-progress functionality
3	Monitor PHP-FPM and web-server worker processes for spawned shells or unexpected child processes
4	Apply file integrity monitoring to web roots and upload directories
5	Track unexpected outbound connections from web servers
6	Review EDR telemetry on PHP hosting servers
7	Monitor the PHP Security Team announcements for the final technical bulletin and updated version guidance
8	Track operating-system, container-image, and hosting-provider channels for patched PHP builds
9	Monitor WAF vendor rule updates addressing these vulnerabilities
10	Retain web-server, WAF, and system logs to support investigation

DISASTER RECOVERY & INCIDENT RESPONSE REQUIREMENTS

Phase	Requirement Area	Actions / Controls
1	Incident Identification	Identify suspected compromise through abnormal requests, new files, or unexpected processes; confirm via WAF, web-server, and EDR logs
2	Immediate Containment	Isolate affected servers; restrict public access; apply WAF protections
3	Evidence Preservation	Preserve web-server, WAF, PHP-FPM, and system logs, suspicious files, and memory/disk images
4	System Recovery	Apply verified PHP patches; remove web shells and persistence; rotate credentials and secrets; restore from known-good backups
5	Post-Incident Actions	Report to National CERT Pakistan; review patch and exposure management processes

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk



National Cyber Emergency Response Team

Government of Pakistan



STRATEGIC PROTECTIVE MEASURES (CII & HIGH-VALUE TARGETS)

1. Treat internet-facing PHP services as priority assets and patch them first once fixes are released.
2. Maintain a current inventory of PHP runtimes, versions, and owners across all environments, including hosting-provider and containerized deployments.
3. Retire or isolate end-of-life PHP deployments that will not receive upstream fixes.
4. Coordinate with hosting providers and managed-service vendors to confirm patch timelines and obtain written validation.
5. Layer WAF protections and continuous monitoring on top of patching rather than relying on any single control.

INCIDENT REPORTING

All incidents related to exploitation of these PHP vulnerabilities, suspected web-shell deployment, or compromise of PHP-hosted services must be reported to National CERT Pakistan:

- **Incident Reporting Portal:** <https://pkcert.gov.pk/report-incident/>
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	PHP has released the fix and all users should update it immediately
2	Inventory all PHP runtimes and identify internet-facing exposure immediately
3	Do not rely on CMS or plugin updates; patch the PHP runtime itself
4	Apply WAF protections and temporary hardening without delaying patching
5	Migrate or isolate end-of-life PHP versions and report incidents to National CERT Pakistan

National Cyber Emergency Response Team (NCERT)

Government of Pakistan

Pak Secretariat, L Block, Islamabad, Pakistan

+92-51-9203422 | info@pkcert.gov.pk | www.pkcert.gov.pk