PAPER TÉCNICO DE CIBERSEGURIDAD

INSTEL & SEGURIDAD
ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

Vulnerabilidades críticas en PHP y alertas de seguridad en Node.js

Investigación de las últimas 72 horas, parches publicados y mitigaciones de contingencia

CVE-2026-109618 · CVE-2026-109619 · Node.js: boletines de julio y octubre 2026

Documento para autoridades, CISOs, administradores de servidores, equipos SOC y responsables de aplicaciones institucionales.

CONTROL DEL DOCUMENTO	DETALLE
Fecha de corte	21 de octubre de 2026, 19:30 ART (22:30 UTC).
Ventana examinada	18/10/2026 19:30 ART – 21/10/2026 19:30 ART (72 h).
Clasificación	Alerta institucional: tratamiento de emergencia P0 para PHP público sin corregir.
Autor	Pedro Matías Cacivio · Perito Informático de la Nación · Instel & Seguridad.
Versión	1.0 · Informe de situación y remediación; sujeto a nuevos avisos oficiales.
Circulación	Responsables de infraestructura y seguridad de organismos públicos y privados.

NOTA DE ALCANCE

Este informe documenta avisos oficiales y recomendaciones técnicas de contención. No implica que las vulnerabilidades se hayan detectado en redes o servidores de ningún organismo concreto. No se ejecutaron pruebas de explotación. La validación final requiere inventario local, evidencia de paquete corregido y comprobación del servicio cargado.

01 | DECISIÓN EJECUTIVA

Resumen ejecutivo y acciones de emergencia

El 21/10/2026 PHP publicó correcciones para dos vulnerabilidades críticas del núcleo del intérprete que permiten ejecución remota de código sin autenticación en escenarios confirmados. Ambas tienen CVSS v4.0 de 9,2. PHP advierte que ninguna mitigación temporal es completa: la única corrección fiable es ejecutar una versión parcheada [S1–S3].

En paralelo, Node.js corrigió diez vulnerabilidades nuevas el 21/10/2026, además de once fallas ya corregidas en julio. El boletín de octubre incluye validación de TLS, DNS, permisos y una escritura fuera de límites en el decodificador Brotli con potencial RCE. Los avisos anteriores de julio se incorporan como antecedentes, NO como vulnerabilidades reveladas durante las últimas 72 horas [S6–S7].

COMPONENTE	VERSIÓN CORREGIDA / MEDIDA
PHP 8.2	8.2.35 o paquete del proveedor que documente ambos parches.
PHP 8.3	8.3.36 o paquete del proveedor con backport confirmado.
PHP 8.4	8.4.27 o paquete del proveedor con backport confirmado.
PHP 8.5	8.5.12 o paquete del proveedor con backport confirmado.
PHP 8.1 y anteriores	Sin mantenimiento ordinario upstream; migrar o validar backport del proveedor.
Node.js 22.x	22.23.4 (LTS).
Node.js 24.x	24.22.1 (LTS).
Node.js 26.x	26.12.1 (Current).

Mandato técnico sugerido para los responsables

01. En las primeras horas: identificar todos los servidores, contenedores, appliances y servicios que emplean PHP o Node.js; priorizar los publicados en Internet y con datos sensibles.

02. Para PHP público no corregido: aplicar parches de emergencia o aislar temporalmente el aplicativo de redes públicas hasta verificar la corrección.

03. Para Node.js: actualizar las ramas 22, 24 y 26 a los builds de octubre; no considerar suficientes las versiones de julio.

04. Preservar registros y evidencias antes de cambios mayores; verificar backup, integridad y procedimiento de reversión.

05. Cerrar cada intervención con evidencia de la versión real del proceso en servicio, boletín del paquete, pruebas funcionales y monitoreo reforzado.

02 | VENTANA TEMPORAL

Hechos comprobados en las últimas 72 horas

FECHA (ART)	EVENTO Y SIGNIFICADO
20 oct	PHP anuncia un parche extraordinario para dos CVE críticas, con publicación prevista para el 21/10 [S1].
21 oct · 10:30	El proyecto PHP libera versiones 8.2.35, 8.3.36, 8.4.27 y 8.5.12. CERT-EU confirma la liberación a las 13:30 UTC [S1, S4].

FECHA (ART)	EVENTO Y SIGNIFICADO
21 oct	Se publican los detalles oficiales de corrupción de memoria OOM y uso de estado global obsoleto; explotación RCE confirmada bajo ciertas condiciones [S2–S3].
21 oct	CERT-EU exige actualización inmediata o aislamiento de aplicaciones públicas cuando no sea posible parchear [S4].
21 oct	Cloudflare informa tráfico de ataque y despliegue de reglas WAF; el proveedor advierte que hay que parchear igualmente [S5].
21 oct	Node.js publica diez nuevas CVE y versiones 22.23.4, 24.22.1 y 26.12.1; incluye actualizaciones de dependencias [S6].

El estudio de las 72 horas cubre el intervalo 18–21/10/2026. La inexistencia de una noticia individual en los días 18 o 19 dentro de las fuentes consultadas NO prueba que no hubiera actividad de ataque. Los once CVE de Node.js publicados en julio se presentan separadamente como contexto histórico.

03 | EVIDENCIA Y LÍMITES

Qué es un hecho confirmado y qué requiere prueba local

CONFIRMADO POR FABRICANTES / CERT	NO DEBE AFIRMARSE SIN VERIFICACIÓN
PHP: existen escenarios de RCE sin autenticación y releases que corrigen ambas CVE.	Que un organismo particular ya fue vulnerado o que todas las rutas de una aplicación son explotables.
Se demostraron vectores en mod_php y, para CVE-2026-109619, también en PHP-FPM.	Que migrar de mod_php a FPM elimine por completo el riesgo.
Cloudflare observó intentos de ataque contra clientes.	Que dichos intentos prueben compromisos exitosos en organizaciones concretas.
Node.js 21/10 publica 10 CVE y builds corregidos.	Que todas las diez fallas afectan idénticamente cada rama y cada uso del runtime.

04 | PHP: DETALLE DE CVE

Mecanismos, prerequisitos e impacto

CVE-2026-109618 — corrupción durante tratamiento de OOM

PHP podía salir anticipadamente mediante longjmp() al fallar una asignación de memoria mientras ciertos datos de la petición todavía no estaban correctamente inicializados. Durante el cierre de la petición, el intérprete podía procesar memoria inválida, permitiendo corrupción de memoria y RCE. Se validó explotación remota sin autenticación contra Apache mod_php, incluso antes de ejecutar código propio de la aplicación. Para PHP-FPM existe exposición plausible por análisis del código, aunque la asesoría de esta CVE no documenta una cadena FPM completa [S2].

CVE-2026-109619 — uso de estado global obsoleto

Determinados estados globales conservaban referencias hacia memoria perteneciente a una petición ya terminada. Un error fatal u otra interrupción podía dejar referencias colgantes y una petición posterior del mismo worker podía utilizarlas antes de que la inicialización normal las reiniciara. El fabricante confirmó divulgación de memoria, use-after-free y RCE sin autenticación; se validaron escenarios en mod_php y PHP-FPM bajo condiciones concretas [S3].

Consecuencias institucionales

- Ejecución con los permisos del worker web, que puede acceder a archivos de configuración y credenciales disponibles para esa cuenta.
- Riesgo de lectura o alteración de bases de datos, movimientos laterales y exposición de información personal si existe conectividad y privilegios suficientes.
- Denegación de servicio por agotamiento de recursos, pérdida de integridad y necesidad de análisis forense ante actividad sospechosa.
- El defecto está en el intérprete PHP: actualizar WordPress, Drupal, Laravel o plugins por sí solo NO corrige estas dos CVE.

05 | PHP: CORRECCIÓN DEFINITIVA

Versiones, ramas heredadas y compatibilidad

RAMA	CORRECCIÓN UPSTREAM	SITUACIÓN
8.5	8.5.12	Seguridad vigente.
8.4	8.4.27	Seguridad vigente.
8.3	8.3.36	Seguridad vigente.
8.2	8.2.35	Recibe seguridad hasta fines de 2026.
<= 8.1	No hay release corriente upstream	Pedir paquete LTS corregido o planificar migración inmediata.

Según CERT-EU, algunos distribuidores y proveedores LTS recibieron parches con antelación y pueden ofrecer correcciones backporteadas; el proyecto también publicó parches mínimos de código fuente para 7.4, 8.0 y 8.1. No hay que calificar un sistema como vulnerable solo porque el número de versión del paquete conserva la rama vieja: deben revisarse el aviso de seguridad y el changelog del proveedor [S4].

Para aplicaciones de hosting administrado o appliances con PHP embebido, el responsable debe solicitar al fabricante la evidencia de corrección. No es prudente reemplazar binarios manualmente en un firmware o equipo soportado sin documentación de compatibilidad.

06 | PHP: CONTENCIÓN TEMPORAL

Mitigaciones recomendadas y sus limitaciones

En toda esta sección se aplica una regla no negociable: las medidas temporales reducen vías conocidas de ataque, pero PHP aclara que solo el parche completo remedia ambas vulnerabilidades [S2–S4].

CONTROL	CONDICIÓN / BENEFICIO	LÍMITE O CONTRAINDICACIÓN
Aislamiento de sitio	Restringir a VPN/IP permitidas o retirar la publicación hasta actualizar.	Puede afectar continuidad; coordinar con el dueño del servicio.
session.upload_progress.enabled=0	Desactiva la vía confirmada de progreso de carga para CVE-109619; reiniciar workers.	No bloquea otros estados globales inseguros; no basta ini_set() ni .user.ini FPM.
fatal_error_backtraces=0	En PHP 8.5 reduce un productor confirmado de estado obsoleto; reiniciar.	No aplica como control general a otras ramas ni elimina otros vectores.
memory_limit=-1	Medida de contingencia indicada por PHP para una vía OOM, aplicada administrativamente.	NO es un ajuste inocuo: puede aumentar consumo/DoS; exige evaluación y límites externos, y tampoco corrige la CVE.
Multipart y límites de carga	Restringir post_max_size, parámetros, cargas, anidamiento y tamaños reales decodificados.	No confiar solo en Content-Length; no evita todas las condiciones.
pm.max_requests=1	Reduce reutilización de memoria entre	Coste alto de rendimiento; no es

CONTROL	CONDICIÓN / BENEFICIO	LÍMITE O CONTRAINDICACIÓN
	peticiones en ciertos FPM; opción defensiva excepcional.	corrección ni sustituto del parche.
WAF actualizado	Añade capacidad de detección/bloqueo; proveedor Cloudflare anunció reglas.	No garantiza cobertura de nuevos bypass ni tráfico interno.

Advertencia explícita del fabricante: no usar RLIMIT_AS o RLIMIT_DATA como sustitutos de los controles de memoria, porque pueden provocar fallos de asignación y activar la ruta vulnerable [S2].

Ejemplo orientativo de directivas para un laboratorio o contingencia revisada por el administrador (no aplicar sin pruebas ni evaluación de funcionalidad):

```
session.upload_progress.enabled = 0

; PHP 8.5 solamente:

; fatal_error_backtraces = 0

; Ajustar a los flujos de carga reales:

post_max_size = 8M
```

Los cambios deben residir en configuración de inicio/administrativa; ejecutar rotación o reinicio controlado de los workers y verificar la configuración EFECTIVA del servidor web. No publicar phpinfo() ni cambiar memory_limit=-1 automáticamente en todos los servidores.

07 | NODE.JS: 72 HORAS

Boletín de seguridad del 21/10/2026 — 10 CVE nuevas

El proyecto Node.js publicó los builds 22.23.4, 24.22.1 y 26.12.1 con soluciones para diez CVE adicionales. La calificación de severidad máxima del boletín es ALTA (HIGH), distinta del CVSS crítico de PHP [S6].

CVE / NIVEL	COMPONENTE Y RIESGO	RAMAS
105482 · ALTA	DNS: truncamiento ante byte NUL en nombre consultado.	22 / 24 / 26
105483 · ALTA	TLS: validación de hostname errónea ante dígitos Unicode fullwidth.	24 / 26
106069 · ALTA	TLS: dirección IP no canónica puede eludir validación de certificado.	22 / 24 / 26
111497 · ALTA	Brotli: escritura fuera de límites; posibilidad de RCE.	22 / 24 / 26
105481 · MEDIA	HTTP keep-alive: manejo incorrecto de respuesta previa a la solicitud.	22 / 24 / 26
106072 · MEDIA	TLS: validación incorrecta frente a formas IPv4 no canónicas.	22 / 24 / 26
106074 · MEDIA	Caches de crypto.randomUUID()/randomInt() reutilizadas en snapshots/SEA.	22 / 24 / 26
106070 · BAJA	ZIP: bytes controlables tras validación fallida de cabecera.	26
106071 · BAJA	Permission Model: ampliación no deseada mediante comodines.	26
106073 · BAJA	Permission Model: evasión mediante fs.realpathSync().	22 / 24 / 26

Todos los identificadores de este cuadro tienen prefijo CVE-2026-. Las ramas citadas corresponden al alcance divulgado por Node.js. La exposición real depende de las APIs y del modelo de despliegue de cada aplicación.

CVE-2026-111497: atención particular al decodificador Brotli

El boletín confirma una escritura fuera de límites en el decodificador Brotli con posibilidad de ejecución remota de código. Se requiere revisar servicios que descomprimen contenido no confiable; no se puede inferir que todo endpoint Node.js sea explotable. Aplicar la versión corregida es la medida prioritaria. Como contención temporal, limitar el procesamiento de flujos comprimidos de origen no confiable donde la arquitectura lo permita, sin asumir protección total [S6].

Actualizaciones complementarias de dependencias

El release de octubre actualiza c-ares y Undici en las tres ramas; incorpora actualización de certificados raíz por el incidente de CA intermedia eMudhra; OpenSSL en 22/24 y SQLite en 22. En los sistemas que usan bibliotecas propias o imágenes empaquetadas, revisar además los avisos del proveedor del entorno [S6–S8].

08 | NODE.JS: CONTEXTO ANTERIOR

Once CVE corregidas el 29/07/2026

Este capítulo aporta contexto para entornos que nunca aplicaron las correcciones de julio; NO se trata de 11 hallazgos nuevos en el periodo de 72 horas. Los builds de julio fueron 22.23.2, 24.18.1 y 26.5.1. Los builds del 21/10 los sustituyen como recomendación de actualización [S7].

CVE / NIVEL	RIESGO PRINCIPAL	RAMAS
56846 · ALTA	HTTP/2: agotamiento remoto de memoria por cabeceras retenidas.	22 / 24
56848 · ALTA	HTTP/2: heap use-after-free (nghttp2).	22 / 24 / 26
58043 · ALTA	Permission Model: acceso a rutas fuera del allowlist.	22 / 24 / 26
56850 · MEDIA	HTTPS Agent: reutilización indebida de identidad mTLS.	22 / 24 / 26
58040 · MEDIA	HTTPS Agent: omisión de verificación de hostname al reusar sesión.	22 / 24 / 26
58041 · MEDIA	SQLite: iterador obsoleto puede reejecutar escrituras.	24 / 26
58042 · MEDIA	DNS: resolución con numerosos registros A termina el proceso.	22 / 24 / 26
58045 · MEDIA	Zlib: longitud simulada de TypedArray puede cerrar el proceso.	22 / 24 / 26
56847 · BAJA	Permission Model: trazas fuera del allowlist.	22 / 24 / 26
58039 · BAJA	Permission Model: reportes fuera del allowlist.	22 / 24 / 26
58044 · BAJA	HTTP: condiciones de request smuggling en proxies específicos.	22 / 24 / 26

Todos los identificadores tienen prefijo CVE-2026-. El uso de --permission no sustituye ACL, permisos POSIX/NTFS, contenedores o ejecución bajo identidades de servicio limitadas.

09 | DIAGNÓSTICO SEGURO

Inventario, aplicación de parches y validación

Identificación local no intrusiva

```
cat /etc/os-release

php -v

php --ini

node -v

ps -eo pid,user,args | grep -E "[p]hp-fpm|[a]pache2|[h]ttpd|[n]ginx|[n]ode"

systemctl list-unit-files | grep -Ei "php|apache|nginx|node"
```

La versión de php -v corresponde a CLI: puede diferir de PHP-FPM, del módulo Apache, del CGI o del PHP dentro de un contenedor. Revisar el binario en ejecución, la configuración del vhost/pool y la evidencia del paquete. En varios hosts conviven distintas ramas y pools.

Secuencia de remediación administrada

01. Antes del cambio: registrar sistema, responsables, aplicación, versión real, proveedor, exposición, copia de seguridad, hash/paquete y procedimiento de vuelta atrás.

02. Verificar el repositorio oficial del sistema o boletín de soporte extendido. En instalaciones manuales o contenedores usar imágenes y artefactos firmados/provenientes del fabricante.

03. Actualizar por medio del gestor de paquetes o pipeline institucional; para PHP reiniciar el servicio/worker que aloja el intérprete; para Node.js reiniciar el proceso y reemplazar todas las réplicas.

04. Verificar la versión efectivamente cargada (no solo el archivo instalado) y revisar changelog/avisos de backport si el número sigue siendo anterior.

05. Efectuar smoke tests autorizados de autenticación, consultas, APIs, cargas, logs y rendimiento, sin PoC público en producción.

06. Cerrar el ticket solo cuando el dueño del servicio confirme funcionamiento y el responsable de seguridad registre evidencia objetiva de corrección.

Comprobaciones en proyectos Node.js

```
node --version

npm --version

npm ls --depth=0

npm audit --json > npm-audit.json

# Revisar manualmente scripts preinstall/install/postinstall

# y validar el lockfile antes de cambiar dependencias
```

npm audit revisa dependencias conocidas; NO prueba que la versión de Node.js esté parcheada ni identifica todo paquete malicioso de reciente publicación. No ejecutar npm audit fix --force de forma automática en producción.

Detección, evidencias e incidentes

Se recomienda aumentar la observabilidad de procesos de PHP-FPM/Apache y Node.js, errores del runtime, conexiones DNS/TLS inesperadas, actividad en WAF, archivos cambiados y procesos secundarios. Ningún evento aislado demuestra explotación de estas CVE. Cloudflare comunicó actividad de ataques en su red, pero ese hecho no acredita intrusión en los sistemas del lector [S5].

ÁMBITO	EVIDENCIAS / SEÑALES A REVISAR
HTTP/WAF	Picos de peticiones multipart; errores 4xx/5xx; cambios de tamaño o cadencia; eventos de reglas de php2shell y correlación de request/response.
PHP	Errores fatales, OOM, fallos de inicialización, reciclado anómalo de workers, diagnósticos INI y upload progress.
Node.js	Caídas, errores de descompresión Brotli, anomalías TLS/DNS, solicitudes externas no esperadas, actividad de snapshots.
Host	Procesos derivados de la cuenta web, cambios en código y directorios temporales, conexiones salientes inusuales y tareas programadas nuevas.
Forense	Conservar logs crudos, zona horaria, reloj, hashes SHA-256, imágenes o snapshots cuando proceda, cadena de custodia y responsable de recolección.

Si se sospecha compromiso

01. Aislar lógicamente el activo y evitar borrados o reinicios innecesarios antes de preservar datos volátiles, conforme a la política del organismo.
02. Capturar evidencias disponibles y reconstruir líneas de tiempo de accesos, procesos, archivos y conexiones; documentar zona horaria y sincronización.
03. Preservar secretos potencialmente expuestos y planificar su rotación en el marco de la contención.
04. Reinstalar o restaurar desde fuente confiable cuando se determine compromiso, actualizar, verificar integridad y vigilar reincidencia.
05. Notificar por los canales internos de respuesta a incidentes y los requerimientos legales aplicables.

11 | PRIORIZACIÓN

Plan operativo recomendado para organismos

PRIORIDAD	SISTEMA	OBJETIVO OPERATIVO PROPUESTO
P0	PHP público no corregido, especialmente mod_php o con acceso a datos sensibles.	Aislar o corregir de inmediato; no esperar a mantenimiento ordinario.
P0	Node.js sin parche que decodifica Brotli no confiable / servicio crítico expuesto.	Actualizar a build de octubre o retirar temporalmente la ruta de riesgo.
P1	Otros PHP públicos y aplicaciones Node.js con DNS/TLS/proxy/permisos afectados.	Corrección acelerada con backup y verificación; seguimiento SOC reforzado.
P2	Intranets y sistemas tras VPN o segmentación robusta.	Ventana controlada lo antes posible, priorizada por datos y acceso.
P3	Laboratorios aislados sin datos reales.	Corregir antes de reconectarlos, clonar

PRIORIDAD	SISTEMA	OBJETIVO OPERATIVO PROPUESTO
		o usarlos como base de producción.

Los niveles P0–P3 y los tiempos de intervención son criterios operativos propuestos por Instel & Seguridad; no reemplazan SLA, categorización CVSS, controles institucionales ni decisiones del comité de continuidad.

Checklist mínimo para cierre institucional

- Inventario completo de las versiones por servicio, contenedor y runtime embebido.
- Identificación y aislamiento de equipos sin parche temporalmente expuestos.
- Paquetes oficiales o backports documentados, pruebas de compatibilidad y reinicios controlados.
- Registro de evidencia: versiones efectivas, changelog, log de actualización, hash y validación del servicio.
- Monitoreo posterior, responsables, fecha de regularización y tratamiento de excepciones.
- Plan de retiro de PHP/Node.js fuera de soporte y revisión de gestión de dependencias y terceros.

12 | DIFUSIÓN INSTITUCIONAL

Texto breve para circular con el paper

ALERTA A RESPONSABLES DE SISTEMAS Y SEGURIDAD: el 21 de octubre de 2026 se publicaron parches urgentes de PHP para CVE-2026-109618 y CVE-2026-109619, que permiten escenarios confirmados de ejecución remota de código sin autenticación (CVSS v4.0 9,2). Deben verificarse y actualizarse de inmediato las instalaciones PHP; donde no sea posible, corresponde evaluar el aislamiento de los sitios públicos. Node.js publicó simultáneamente actualizaciones de seguridad para ramas 22, 24 y 26, incluyendo una falla de posible RCE en Brotli. Se solicita inventario, verificación de versiones del proceso en ejecución, conservación de evidencias, actualización desde proveedor oficial y comunicación del estado de cumplimiento a la unidad de seguridad. El WAF y otras medidas de contención NO reemplazan los parches.

13 | FUENTES Y TRAZABILIDAD

Referencias principales consultadas

[S1] PHP – News Archive, releases del 20 y 21 de octubre de 2026. https://www.php.net/archive/2026.php

[S2] PHP Security Advisory GHSA-w8hw-w9fx-j79w: CVE-2026-109618. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

[S3] PHP Security Advisory GHSA-6wmf-4rv5-p3rp: CVE-2026-109619. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp

[S4] CERT-EU Security Advisory 2026-018 (21/10/2026). https://cert.europa.eu/publications/security-advisories/2026-018

[S5] Cloudflare: WAF protections against php2shell (21/10/2026). https://blog.cloudflare.com/php-vulnerabilities-waf-protection

[S6] Node.js: Wednesday, October 21, 2026 Security Releases. https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

[S7] Node.js: Wednesday, July 29, 2026 Security Releases. https://nodejs.org/en/blog/vulnerability/july-2026-security-releases

[S8] Node.js: notas de versión de 22.23.4, 24.22.1 y 26.12.1. https://nodejs.org/en/blog/release/v24.22.1/

[S9] NCSC-NL: repositorio institucional php2shell. https://github.com/NCSC-NL/php2shell

[S10] NCSC Reino Unido: Critical security issue affecting PHP. https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php

Criterio de atribución: las fuentes primarias PHP/Node.js, CERT-EU y los comunicados de proveedores son la base de los hallazgos técnicos. Noticias periodísticas y comunicaciones externas no son prueba de compromiso de un activo institucional. La ausencia de explotación observada no demuestra inmunidad.

Escrito por: PEDRO MATÍAS CACIVIO | Perito Informático de la Nación | Instel & Seguridad

Documento técnico para difusión entre equipos de infraestructura y ciberseguridad. No sustituye la verificación sobre cada entorno ni autoriza pruebas intrusivas.