

Nro. Alerta:	AL-2026-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP: CLEAR 		
Fecha:	21-oct-2026	ALERTAS DE SEGURIDAD PHP2Shell – Vulnerabilidades críticas que permiten ejecución remota de código en PHP	V 1.1 Pág.: 1 of 4

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades
Tipo de Incidente: Ejecución remota de código (RCE)
Nivel de riesgo: Alta

II. ALERTA



Figura 1.- PHP2Shell – Vulnerabilidades críticas que permiten ejecución remota de código en PHP - figura referencial

Se identifican dos vulnerabilidades críticas en PHP que podrían comprometer la seguridad de servidores y aplicaciones web que utilicen versiones afectadas. Se recomienda a las organizaciones verificar sus sistemas y aplicar las actualizaciones de seguridad correspondientes.

III. INTRODUCCIÓN

PHP es un lenguaje de programación ampliamente utilizado en el desarrollo de aplicaciones y servicios web. Las vulnerabilidades identificadas como CVE-2026-109618 y CVE-2026-109619 afectan mecanismos internos relacionados con la gestión de memoria y el procesamiento de solicitudes.

La explotación de estas fallas podría permitir a un atacante remoto ejecutar código sin autenticación previa en determinadas configuraciones. Aunque se ha informado sobre la circulación inicial de pruebas de concepto (PoC), la información disponible no confirma ataques exitosos en entornos reales.

Nro. Alerta:	AL-2026-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	21-oct-2026	PHP2Shell – Vulnerabilidades críticas que permiten ejecución remota de código en PHP	V 1.1 Pág.: 2 of 4

IV. VECTOR DE ATAQUE

El ataque podría realizarse de forma remota mediante el envío de solicitudes HTTP especialmente manipuladas a un servidor que ejecute una versión vulnerable de PHP. En determinados escenarios, la explotación podría ocurrir antes de que se procese el código propio de la aplicación.

Las vulnerabilidades se relacionan con dos condiciones:

- **CVE-2026-109618:** manejo incorrecto de la memoria durante errores de agotamiento de recursos (*Out-of-Memory*, OOM).
- **CVE-2026-109619:** utilización de información interna residual entre solicitudes procesadas por un mismo trabajador.

Entre los componentes que deben revisarse se encuentran PHP-FPM, Apache con mod_php, PHP-CGI, FrankenPHP y LiteSpeed. La exposición y las posibilidades de explotación dependen de la versión instalada y de la configuración del entorno.

V. IMPACTO

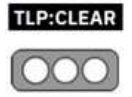
Producto	Versiones afectadas	Versión corregida
PHP 8.5	Anteriores a 8.5.12	8.5.12
PHP 8.4	Anteriores a 8.4.27	8.4.27
PHP 8.3	Anteriores a 8.3.36	8.3.36
PHP 8.2	Anteriores a 8.2.35	8.2.35
PHP 8.1 y anteriores	Versiones sin soporte; verificar con el proveedor	Actualizar a una versión compatible y corregida

Tabla 1.- Productos y versiones afectadas por las vulnerabilidades PHP2Shell.

VI. INDICADORES DE COMPROMISO

No se dispone de indicadores específicos confirmados, como direcciones IP, dominios o hashes, asociados directamente con la explotación de estas vulnerabilidades. Para identificar posibles incidentes, se recomienda revisar:

- **Registros web y de proxy:** solicitudes HTTP inusuales, cargas de archivos atípicas y peticiones que generen errores repetitivos.
- **Registros de PHP y del servidor:** errores de agotamiento de memoria, fallos fatales y reinicios inesperados de procesos.

Nro. Alerta:	AL-2026-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	 V 1.1
TLP:			
Fecha:	21-oct-2026	PHP2Shell – Vulnerabilidades críticas que permiten ejecución remota de código en PHP	Pág.: 3 of 4

- **Procesos del sistema:** ejecución inesperada de intérpretes de comandos, procesos secundarios no habituales o conexiones salientes sospechosas.
- **Integridad de archivos:** cambios no autorizados en archivos web, configuraciones, scripts o tareas programadas.
- **Acceso a información:** lecturas inusuales de archivos de configuración, credenciales u otros datos sensibles.

Estos elementos son señales para la investigación técnica y no constituyen, por sí solos, evidencia de explotación.

VII. RECOMENDACIONES:

- Actualizar PHP a una versión corregida compatible con el entorno: 8.5.12, 8.4.27, 8.3.36 o 8.2.35, o instalar el parche oficial correspondiente proporcionado por el proveedor.
- Identificar todas las instalaciones de PHP que procesan solicitudes web, incluidas las integradas en contenedores, paneles de control y aplicaciones de terceros.
- Priorizar la revisión de servidores expuestos a Internet y de configuraciones que utilicen Apache con mod_php.
- Si la actualización inmediata no es posible, aplicar únicamente las mitigaciones temporales documentadas por PHP o por el proveedor del sistema, entendiendo que no sustituyen la instalación del parche.
- Revisar los registros de acceso web y del sistema para identificar solicitudes sospechosas, errores anómalos y posibles señales de ejecución de comandos.
- Verificar la integridad de los archivos web y revisar procesos, tareas programadas y cuentas que presenten actividad inusual.
- Reiniciar los procesos o servicios PHP afectados después de aplicar las actualizaciones, según las instrucciones del proveedor.
- Mantener copias de seguridad actualizadas y comprobar que sea posible restaurarlas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

Nro. Alerta:	AL-2026-056	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	21-oct-2026	ALERTAS DE SEGURIDAD PHP2Shell – Vulnerabilidades críticas que permiten ejecución remota de código en PHP	V 1.1 Pág.: 4 of 4

IX. REFERENCIAS:

THE HACKER NEWS. (2026). PHP2Shell: What Actually Protects You? [\[https://thehacker-news.com/2026/10/php2shell-what-actually-protects-you.html?m=1\]](https://thehacker-news.com/2026/10/php2shell-what-actually-protects-you.html?m=1)

PHP. (2026). PHP 2026 Changelog and Security Releases. [\[https://www.php.net/archive/2026.php#2026-10-20-1\]](https://www.php.net/archive/2026.php#2026-10-20-1)

PHP2SHELL. (2026). PHP2Shell – Critical PHP Vulnerabilities. [\[https://www.php2shell.com/\]](https://www.php2shell.com/)

ADEMKING. (2026). PHP2Shell Nuclei Templates. GitHub. [\[https://github.com/Ademking/php2shell-nuclei-templates\]](https://github.com/Ademking/php2shell-nuclei-templates)