Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA DE EJECUCIÓN REMOTA DE CÓDIGO (CVE-2025-24016) AFECTA

13 / 02 / 2025

CONTENIDO

INTRODUCCIÓN

La vulnerabilidad CVE-2025-24016 en Wazuh, con un CVSS de 9.9, permite la ejecución remota de código debido a una deserialización insegura en la API del servidor. Afecta a todas las versiones anteriores a la 4.9.1, con ataques confirmados en 4.8.0, 4.7.2 y 4.6.1. Un atacante con acceso a la API puede comprometer el sistema enviando solicitudes maliciosas. Se recomienda actualizar a la versión 4.9.1, auditar accesos, restringir permisos y reforzar la seguridad de los agentes para mitigar el riesgo de explotación.

VULNERABILIDAD CRÍTICA DE EJECUCIÓN REMOTA DE CÓDIGO (CVE-2025-24016) AFECTA A WAZUH

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_02_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/02/2025
Es día cero (0 day):	No

RESUMEN

El equipo de Wazuh ha emitido una alerta de seguridad sobre una grave vulnerabilidad en su plataforma de seguridad. Identificada como CVE-2025-24016, esta falla ha recibido un puntaje de 9.9 en el sistema CVSS, lo que la clasifica como crítica. La vulnerabilidad permite a un atacante ejecutar código de manera remota en servidores afectados, comprometiendo por completo su integridad y seguridad.

Detalles técnicos

Wazuh es una solución open-source utilizada para detección de amenazas, monitoreo de integridad de archivos, análisis de logs y respuesta ante incidentes. Sin embargo, CVE-2025-24016 explota una falla de deserialización insegura en la API del servidor Wazuh, permitiendo que un atacante ejecute comandos arbitrarios mediante el envío de una solicitud especialmente diseñada.

Según el aviso de seguridad, el ataque puede ser llevado a cabo por cualquier usuario con acceso a la API de Wazuh, incluyendo actores malintencionados que hayan comprometido el dashboard o algún nodo del clúster. En ciertas configuraciones, también es posible que un agente comprometido desencadene la explotación.

Prueba de concepto (PoC)

Se ha publicado un exploit de prueba de concepto (PoC) que muestra la facilidad con la que se puede explotar esta vulnerabilidad para apagar un servidor maestro:

curl -X POST -k -u "wazuh-wui:MyS3cr37P450r.-" -H "Content-Type: application/json" --data '{"__unhandled_exc__":{"__class__": "exit", "__args__": []}}' https://<worker-server>:55000/security/user/authenticate/run_as*

Este ataque demuestra la gravedad de la vulnerabilidad, especialmente en configuraciones con credenciales por defecto o insuficientemente protegidas.

Versiones afectadas

Se ha confirmado que los atacantes han explotado activamente las versiones 4.4.0, 4.7.2 a la 4.9.1, lo que aumenta la urgencia de actualizar a la versión corregida.

Solución y mitigación

Para mitigar esta vulnerabilidad, se recomienda encarecidamente que todos los administradores actualicen sus servidores a la versión 4.9.1 de Wazuh, donde se ha corregido este problema.

Pasos para actualizar:

- Descargar la nueva versión desde el sitio oficial de Wazuh.
- Seguir las instrucciones de actualización proporcionadas por el equipo de Wazuh.
- Revisar las configuraciones de seguridad de la API y los permisos de acceso.
- Implementar medidas de endurecimiento (hardening) en los agentes para minimizar la exposición.

Conclusión

Dado el impacto potencial de CVE-2025-24016, es crucial que las organizaciones que utilizan Wazuh tomen medidas inmediatas para proteger sus infraestructuras. Además de actualizar a la versión 4.9.1, se recomienda auditar y restringir el acceso a la API del servidor y aplicar buenas prácticas de seguridad para minimizar el riesgo de futuras explotaciones.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-de-ejecucion-remota-de-codigo-cve-2025-24016-afecta-a-wazuh/

CONTACTOS DE SOPORTE

Correo electrónico: info@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/