Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FORTINET ADVIERTE SOBRE NUEVA VULNERABILIDAD ZERO-DAY UTILIZADA PARA

11 / 02 / 2025

CONTENIDO

INTRODUCCIÓN

Fortinet ha emitido una alerta de seguridad sobre una nueva vulnerabilidad zero-day, identificada como CVE-2025-24472, que está siendo explotada activamente por ciberdelincuentes para comprometer firewalls FortiGate y acceder a redes empresariales. Esta vulnerabilidad permite a los atacantes obtener privilegios de superadministrador a través de solicitudes maliciosas al proxy CSF, lo que les otorga un control total sobre los dispositivos afectados. Ante esta amenaza, es crucial que las organizaciones tomen medidas inmediatas para mitigar el riesgo y proteger sus infraestructuras críticas.

FORTINET ADVIERTE SOBRE NUEVA VULNERABILIDAD ZERO-DAY UTILIZADA PARA SECUESTRAR FIREWALLS

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

ID de alerta:	DSOC-CERT_2025_02_11_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	11/02/2025
Es día cero (0 day):	SÍ

RESUMEN

Fortinet ha alertado a sus clientes sobre una nueva vulnerabilidad zero-day que está siendo explotada activamente para comprometer firewalls FortiGate y acceder a redes empresariales. El fallo de seguridad, identificado como **CVE-2025-24472**, permite a atacantes remotos obtener privilegios de superadministrador mediante solicitudes maliciosas al proxy CSF.

La vulnerabilidad afecta a **FortiOS** en sus versiones **7.0.0 a 7.0.16** y **FortiProxy** en sus versiones **7.0.0 a 7.0.19** y **7.2.0 a 7.2.12**. **Fortinet añadió este CVE** a un aviso de seguridad previo en el que advertía sobre otra vulnerabilidad de autenticación (**CVE-2024-55591**), que puede ser explotada mediante solicitudes maliciosas al módulo websocket de Node.js.

Ataques en curso y posibles impactos

Los ciberdelincuentes están aprovechando ambas vulnerabilidades para generar cuentas de administrador o usuarios locales en dispositivos comprometidos, integrándolos en grupos de usuarios SSL VPN nuevos o ya existentes. También han sido detectadas modificaciones en políticas de firewall y configuraciones críticas, así como el uso de cuentas fraudulentas para establecer túneles hacia la red interna.

Se ha confirmado que firewalls FortiGate con interfaces de administración expuestas a Internet han sido blanco de ataques desde **mediados de noviembre de 2024**. Según los informes, los ataques se han desarrollado en varias fases:

- **Exploración de vulnerabilidades** (16 al 23 de noviembre de 2024)
- **Reconocimiento** (22 al 27 de noviembre de 2024)
- **Configuración de SSL VPN** (4 al 7 de diciembre de 2024)
- **Movimiento lateral** dentro de las redes afectadas (16 al 27 de diciembre de 2024)

Los investigadores han detectado diferencias en las tácticas y en la infraestructura utilizada, lo que sugiere la posible participación de múltiples actores de amenazas. Sin embargo, el uso de la herramienta **jsconsole** fue un elemento común en los ataques.

Recomendaciones de Fortinet

Para mitigar el riesgo de explotación, Fortinet recomienda a las organizaciones que no puedan aplicar inmediatamente las actualizaciones de seguridad:

- **Deshabilitar el acceso a la interfaz administrativa HTTP/HTTPS** en los firewalls afectados.
- **Restringir el acceso** a la interfaz de administración mediante políticas de acceso local.
- **Aplicar las actualizaciones de seguridad** tan pronto como estén disponibles.

Se notificó a Fortinet sobre la actividad maliciosa el 12 de diciembre de 2024, y la compañía confirmó la investigación cinco días después.

Solución a las vulnerabilidades

Fortinet ha lanzado parches de seguridad que solucionan estas vulnerabilidades. Se recomienda a todas las organizaciones actualizar a las últimas versiones de **FortiOS y FortiProxy** de inmediato. Además, se debe auditar la configuración del firewall, eliminar cuentas sospechosas y revisar los registros de acceso para detectar cualquier actividad inusual.

Conclusión

Este incidente subraya la importancia de mantener una postura de seguridad proactiva, especialmente cuando se trata de dispositivos perimetrales expuestos a Internet. Las organizaciones deben asegurarse de implementar controles de acceso adecuados y aplicar parches de seguridad de manera oportuna para mitigar el riesgo de explotación de vulnerabilidades zero-day.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/d3f0d91fe4975240011107873d0ae8dc9aa47b1a/CVE-2025-24472

NOTICIA COMPLETA

https://devel.group/blog/fortinet-advierte-sobre-nueva-vulnerabilidad-zero-day-utilizada-para-secuestrar-firewalls/

CONTACTOS DE SOPORTE

Correo electrónico: info@devel.group

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/