BEACON LAB
C S I R T

CYBOLT
Security Innovation

# Boletín de Alerta

Boletín Nro.: 2025-04
Fecha de publicación: 14/01/2025
Tema: Vulnerabilidad crítica explotada activamente en firewalls Fortinet

Traffic Light Protocol (TLP): White


## Producto(s) afectado(s):

- FortiOS versiones 7.0.0 a 7.0.16
- FortiProxy versiones 7.0.0 a 7.0.19 y 7.2.0 a 7.2.12

## Descripción

Fortinet ha emitido una alerta sobre una vulnerabilidad de día cero (ZeroDay) identificada como **CVE-2024-55591** con un puntaje **CVSS de 9.6,** que permite la omisión de autenticación en sus productos FortiOS y FortiProxy. Existen reportes que dicen que dicha vulnerabilidad estan siendo explotadas activamente para comprometer firewalls y acceder a redes empresariales.

La vulnerabilidad CVE-2024-55591, permite a atacantes remotos obtener privilegios de superadministrador mediante solicitudes maliciosas al módulo websocket de Node.js. Los atacantes han utilizado esta falla para crear usuarios administrativos no autorizados, modificar políticas de firewall y acceder a redes internas a través de SSL VPN. El problema radica en el manejo inadecuado de las solicitudes enviadas al módulo websocket utilizado en la interfaz de administración.

Diche vulnerabilidad se puede explotar remotamente desde el Internet, sin necesidad de estar autenticado.  Esto es un gran riego especialmente para la organización que tienen la interfaz web expuesta a Internet.

Fortinet ha confirmado que esta vulnerabilidad ya está siendo utilizada en ataques dirigidos. Los incidentes registrados incluyen la toma de control completo de firewalls, lo que podría ser parte de campañas de ciberespionaje o intrusiones de alto perfil.

La vulnerabilidad impacta a las versiones de FortiOS entre **7.0.0 y 7.0.16**, así como a FortiProxy entre **7.0.0 y 7.0.19** y **7.2.0 y 7.2.12**. Los dispositivos con interfaces de administración expuestas públicamente son particularmente vulnerables a los ataques.

Se estima que hay alrededor 24000 dispositivos Fortinet en México conectados actualmente.

## Solución

Fortinet ha lanzado actualizaciones de seguridad para corregir esta vulnerabilidad. Se recomienda a todos los usuarios actualizar sus dispositivos a las versiones más recientes de FortiOS y FortiProxy de inmediato. Además, se aconseja revisar las configuraciones de seguridad, monitorear la creación de cuentas sospechosas y restringir el acceso a las interfaces de administración web expuestas a Internet, si es necesario publicarlo por cuestion operativas, hacerlo a traves de una VPN restringida.

Para mas detalles sobre la vulnerabilidad puede consultar el siguiente enlace:
https://fortiguard.fortinet.com/psirt/FG-IR-24-535

Para acceder a las actualizaciones, puede seguir el siguiente enlace:.
https://docs.fortinet.com/upgrade-tool/fortigate

## Información adicional:

- https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/
- https://www.bleepingcomputer.com/news/security/fortinet-warns-of-auth-bypass-zero-day-exploited-to-hijack-firewalls/
- https://fortiguard.fortinet.com/psirt/FG-IR-24-535
- https://docs.fortinet.com/upgrade-tool/fortigate

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com