Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD ZERO-DAY EN FIREWALLS FORTINET FORTIGATE

15 / 01 / 2025

CONTENIDO

INTRODUCCIÓN....3
RESUMEN....5
NOTICIA COMPLETA....6
CONTACTOS DE SOPORTE....7

INTRODUCCIÓN

Una reciente actividad maliciosa ha expuesto la vulnerabilidad crítica CVE-2024-55591 en dispositivos Fortinet FortiGate y FortiProxy con interfaces de administración expuestas a internet, resaltando la constante amenaza que representan los ataques Zero-Day. Desde noviembre de 2024, actores malintencionados han explotado esta debilidad para acceder a configuraciones, crear cuentas de superadministrador y extraer credenciales mediante técnicas avanzadas como DCSync. Este incidente subraya la importancia de mantener firmware actualizado, restringir accesos no autorizados y adoptar medidas proactivas de ciberseguridad para proteger dispositivos críticos en un entorno cada vez más complejo y dinámico

VULNERABILIDAD ZERO-DAY EN FIREWALLS FORTINET FORTIGATE

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

ID de alerta:	DSOC-CERT_2025_01_15_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	15/01/2025
Es día cero (0 day):	Sí

RESUMEN

En el ámbito de la ciberseguridad, una reciente actividad maliciosa ha puesto en jaque a los dispositivos firewall Fortinet FortiGate con interfaces de administración expuestas en internet. Identificada como una vulnerabilidad de tipo Zero-Day, esta amenaza pone de manifiesto la importancia de mantener una configuración de seguridad robusta en las organizaciones.

Ataques Dirigidos a Firewalls con Interfaces Expuestas

Los investigadores han detectado actividades maliciosas que comenzaron a mediados de noviembre de 2024, donde actores desconocidos accedieron a interfaces de administración para alterar configuraciones y extraer credenciales utilizando la técnica DCSync. Estos ataques involucraron:

- **Creación de cuentas de administrador superusuario.**
- **Autenticaciones SSL VPN mediante cuentas comprometidas.**
- **Cambios en configuraciones clave de los firewalls.**

El acceso inicial, aunque aún no confirmado, apunta con alta confianza al uso de una vulnerabilidad Zero-Day. Esto se infiere por la rapidez con la que varias organizaciones y versiones de firmware resultaron afectadas.

Fases del Ataque

La actividad avanzó en cuatro etapas bien definidas:

1. **Reconocimiento inicial y exploración de vulnerabilidades.**
2. **Modificaciones en configuraciones y creación de cuentas.**
3. **Configuración de portales SSL VPN y tunelado de accesos.**
4. **Extracción de credenciales para movimiento lateral.**

Cabe destacar el uso extensivo de la interfaz “jsconsole” desde un número limitado de direcciones IP sospechosas, lo que subraya la sofisticación y coordinación de los atacantes.

Confirmación de Fortinet: Vulnerabilidad Crítica

El 14 de enero de 2025, Fortinet publicó detalles sobre una vulnerabilidad de omisión de autenticación (CVE-2024-55591) con un puntaje CVSS de 9.6. Este fallo permite a atacantes remotos obtener privilegios de superadministrador mediante solicitudes manipuladas al módulo websocket de Node.js.

- **FortiOS 7.0.0 a 7.0.16** (actualizar a 7.0.17 o superior).
- **FortiProxy 7.0.0 a 7.0.19** (actualizar a 7.0.20 o superior).
- **FortiProxy 7.2.0 a 7.2.12** (actualizar a 7.2.13 o superior).

Fortinet también confirmó que esta vulnerabilidad ha sido utilizada para crear cuentas, modificar grupos de usuarios y alterar políticas de firewall.

Recomendaciones de Mitigación

Para reducir los riesgos asociados a esta vulnerabilidad, las organizaciones deben:

1. **Actualizar inmediatamente el firmware afectado a las versiones recomendadas por Fortinet.**
2. **Evitar exponer las interfaces de administración de firewalls a internet.**
3. **Implementar listas de control de acceso (ACL) para limitar conexiones a usuarios confiables.**

4. **Auditar cuentas y configuraciones regularmente para detectar actividades sospechos**as.

Impacto y Lecciones Aprendidas

Esta actividad no se limitó a sectores o tamaños específicos de organizaciones, lo que sugiere un enfoque oportunista por parte de los atacantes. El uso de eventos automatizados de inicio y cierre de sesión subraya la necesidad de fortalecer las medidas de seguridad en torno a dispositivos críticos.
En un panorama donde las vulnerabilidades Zero-Day representan una amenaza constante, es esencial priorizar actualizaciones, implementar buenas prácticas de configuración y fomentar una cultura de ciberseguridad proactiva.

Versiones afectadas:

- **FortiOS 7.0.0 a 7.0.16** (actualizar a 7.0.17 o superior).
- **FortiProxy 7.0.0 a 7.0.19** (actualizar a 7.0.20 o superior).
- **FortiProxy 7.2.0 a 7.2.12** (actualizar a 7.2.13 o superior).

Fortinet también confirmó que esta vulnerabilidad ha sido utilizada para crear cuentas, modificar grupos de usuarios y alterar políticas de firewall.

Recomendaciones de Mitigación

Para reducir los riesgos asociados a esta vulnerabilidad, las organizaciones deben:

1. **Actualizar inmediatamente el firmware afectado a las versiones recomendadas por Fortinet.**
2. **Evitar exponer las interfaces de administración de firewalls a internet.**
3. **Implementar listas de control de acceso (ACL) para limitar conexiones a usuarios confiables.**
4. **Auditar cuentas y configuraciones regularmente para detectar actividades sospechosas.**

Impacto y Lecciones Aprendidas

Esta actividad no se limitó a sectores o tamaños específicos de organizaciones, lo que sugiere un enfoque oportunista por parte de los atacantes. El uso de eventos automatizados de inicio y cierre de sesión subraya la necesidad de fortalecer las medidas de seguridad en torno a dispositivos críticos.
En un panorama donde las vulnerabilidades Zero-Day representan una amenaza constante, es esencial priorizar actualizaciones, implementar buenas prácticas de configuración y fomentar una cultura de ciberseguridad proactiva.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-zero-day-en-firewalls-fortinet-fortigate/

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://www.devel.group/