Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

UNA FALLA CRÍTICA PONE EN RIESGO LA SEGURIDAD DE FORTISWITCH

08 / 04 / 2025

CONTENIDO

INTRODUCCIÓN

Fortinet ha emitido una alerta de seguridad tras descubrir una vulnerabilidad crítica en la interfaz gráfica de FortiSwitch, uno de sus productos clave en redes empresariales. La falla permite a atacantes remotos no autenticados modificar contraseñas administrativas, lo que representa un riesgo significativo para la integridad de los entornos corporativos. Aunque no se han reportado casos de explotación activa, Fortinet recomienda aplicar las actualizaciones disponibles con urgencia y adoptar medidas de mitigación mientras se implementan los parches.

UNA FALLA CRÍTICA PONE EN RIESGO LA SEGURIDAD DE FORTISWITCH

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

ID de alerta:	DSOC-CERT_2025_04_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/04/2025
Es día cero (0 day):	No

RESUMEN

Fortinet, proveedor líder en soluciones de ciberseguridad, ha emitido una alerta para que los usuarios actualicen sus dispositivos FortiSwitch, luego de descubrirse una vulnerabilidad crítica que podría permitir a atacantes remotos cambiar contraseñas de administrador sin autenticación previa.

La vulnerabilidad ha sido identificada como CVE-2024-48887 y ha recibido un puntaje CVSS de 9.3 sobre 10, lo que la clasifica como una amenaza de alto impacto.

¿En qué consiste la vulnerabilidad?

Según el aviso oficial de Fortinet, se trata de una llamada CWE-620: Unverified Password Change, localizada en la interfaz gráfica de usuario (GUI) de FortiSwitch. Esta brecha permite que un atacante remoto no autenticado pueda modificar las contraseñas administrativas simplemente mediante el envío de una solicitud especialmente diseñada.

La vulnerabilidad fue detectada internamente por el equipo de desarrollo de la interfaz web de FortiSwitch.

Versiones afectadas y actualizaciones recomendadas

Los dispositivos FortiSwitch afectados abarcan varias versiones del firmware. A continuación, se detallan las versiones vulnerables y sus respectivas recomendaciones de actualización:

- FortiSwitch 7.6.0 → actualizar a 7.6.1 o superior
- FortiSwitch 7.4.0 – 7.4.4 → actualizar a 7.4.5 o superior
- FortiSwitch 7.2.0 – 7.2.8 → actualizar a 7.2.9 o superior
- FortiSwitch 7.0.0 – 7.0.10 → actualizar a 7.0.11 o superior
- FortiSwitch 6.4.0 – 6.4.14 → actualizar a 6.4.15 o superior

Recomendaciones de mitigación inmediata

Aunque no se han detectado casos de explotación activa de esta vulnerabilidad, Fortinet ha proporcionado medidas de mitigación temporal para quienes aún no puedan aplicar el parche de seguridad:

Desactivar el acceso HTTP/HTTPS desde las interfaces administrativas.

Restringir el acceso únicamente a hosts de confianza.

Riesgos de no aplicar el parche

Históricamente, múltiples vulnerabilidades en productos de Fortinet han sido aprovechadas por actores maliciosos para campañas de ciberataques, por lo que es crucial actuar de inmediato para evitar brechas de seguridad.

Conclusión

Las empresas que utilicen FortiSwitch deben tomar medidas proactivas para actualizar sus sistemas y revisar sus políticas de acceso administrativo. La ciberseguridad no solo depende de las herramientas que se implementen, sino también del compromiso constante con el mantenimiento y actualización de estas.

NOTICIA COMPLETA

https://devel.group/blog/una-falla-critica-pone-en-riesgo-la-seguridad-de-fortiswitch/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@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/