Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA EN FORTIMANAGER: CIBERCRIMINALES APROVECHAN FALLO DE AUTENTICACIÓN PARA EJECUTAR CÓDIGO REMOTO

23 / 10 / 2024

c

CONTENIDO

INTRODUCCIÓN

Fortinet ha revelado una grave vulnerabilidad en su plataforma de gestión FortiManager, la cual permite a atacantes remotos no autenticados ejecutar código o comandos arbitrarios. Esta vulnerabilidad, relacionada con una falla de autenticación en el Demon de fgfmd, está siendo activamente explotada, lo que pone en riesgo la seguridad de redes corporativas al facilitar la exfiltración de datos sensibles, como credenciales e información de configuración de dispositivos gestionados. Las organizaciones afectadas deben actualizar inmediatamente sus sistemas a las versiones corregidas y aplicar las mitigaciones recomendadas para protegerse de posibles ataques.

VULNERABILIDAD CRÍTICA EN FORTIMANAGER: CIBERCRIMINALES APROVECHAN FALLO DE AUTENTICACIÓN PARA EJECUTAR CÓDIGO REMOTO

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

ID de alerta:	DSOC-CERT_2024_10_23_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	23/10/2024
Es día cero (0 day):	SÍ

RESUMEN

Recientemente, se ha identificado una vulnerabilidad crítica en FortiManager, un sistema clave para la gestión centralizada de dispositivos Fortinet, que permite a cibercriminales ejecutar código o comandos arbitrarios de manera remota. Este fallo, relacionado con la falta de autenticación para funciones críticas (CWE-306) en el Demon de fgfmd de FortiManager, está siendo explotado activamente en la naturaleza, lo que aumenta el riesgo de compromisos severos en las redes corporativas.

Versión afectada y solución disponible

La vulnerabilidad afecta a múltiples versiones de FortiManager y FortiManager Cloud. A continuación, se listan las versiones afectadas y las soluciones recomendadas por Fortinet:

- FortiManager 7.6: Afecta la versión 7.6.0; se recomienda actualizar a la versión 7.6.1 o superior.
- FortiManager 7.4: Afecta las versiones de 7.4.0 a 7.4.4; se recomienda actualizar a la versión 7.4.5 o superior.
- FortiManager 7.2: Afecta las versiones de 7.2.0 a 7.2.7; se recomienda actualizar a la versión 7.2.8 o superior.
- FortiManager 7.0: Afecta las versiones de 7.0.0 a 7.0.12; se recomienda actualizar a la versión 7.0.13 o superior.
- FortiManager 6.4: Afecta las versiones de 6.4.0 a 6.4.14; se recomienda actualizar a la versión 6.4.15 o superior.
- FortiManager 6.2: Afecta las versiones de 6.2.0 a 6.2.12; se recomienda actualizar a la versión 6.2.13 o superior.
- FortiManager Cloud: Algunas versiones de 7.4 y 7.2 están afectadas; se recomienda migrar o actualizar según el caso.

Impacto y recomendaciones

Las versiones de FortiManager afectadas permiten que un atacante no autenticado envíe solicitudes especialmente diseñadas para ejecutar comandos maliciosos en el sistema. Los informes indican que esta vulnerabilidad ya ha sido explotada activamente en el entorno salvaje, con ataques centrados en la exfiltración de archivos que contienen IPs, credenciales y configuraciones de dispositivos gestionados.

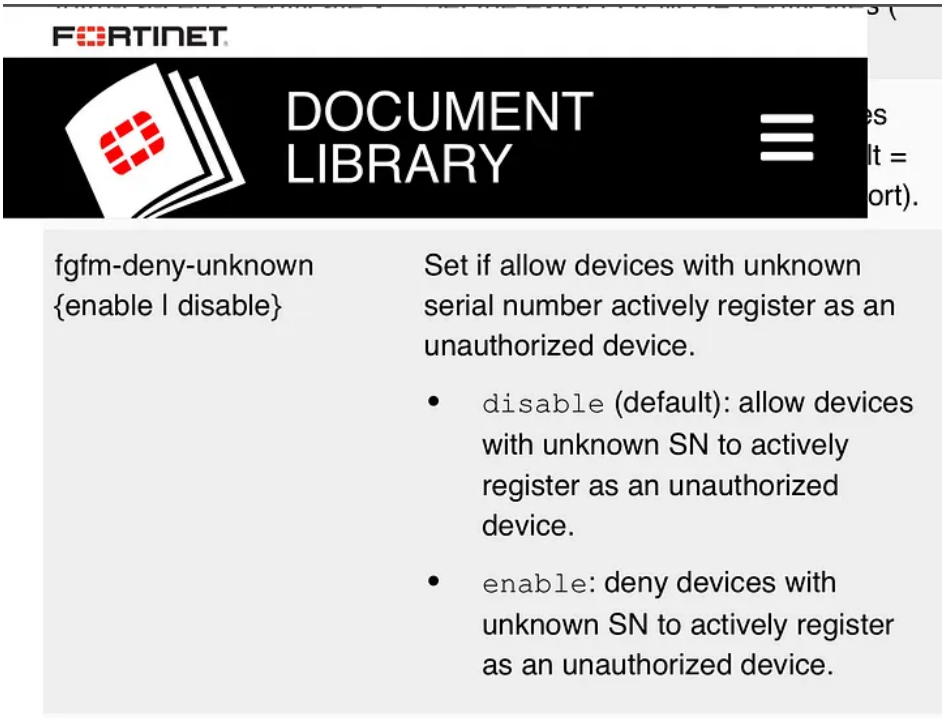
Además, ciertos modelos antiguos de FortiAnalyzer, cuando tienen habilitada la función FortiManager, también son vulnerables. Entre ellos están los modelos 1000E, 1000F, 2000E, 3000E/F/G, y otros.

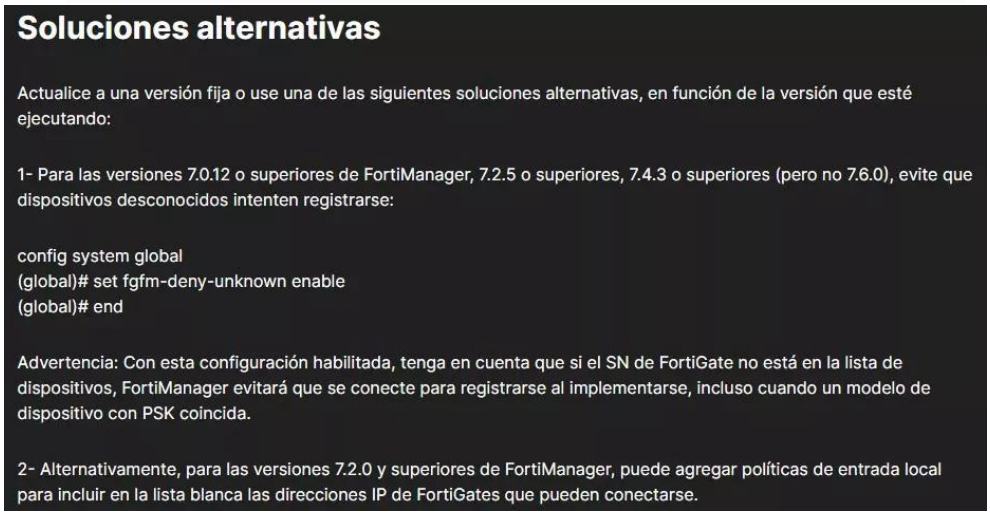
Fortinet ha proporcionado varias alternativas de mitigación

- Actualizar a las versiones parcheadas indicadas.
- Configurar políticas locales para permitir solo direcciones IP autorizadas de dispositivos FortiGate.
- Implementar certificados personalizados para autenticar dispositivos gestionados.

Hasta el momento, no se han detectado instaladores de malware de bajo nivel o puertas traseras en los sistemas comprometidos. Sin embargo, se recomienda a las organizaciones afectadas que cambien las

credenciales de todos los dispositivos gestionados y revisen cuidadosamente la configuración de FortiManager para detectar modificaciones no autorizadas.





Recuperación

Fortinet sugiere realizar copias de seguridad de la configuración del FortiManager antes de la identificación de indicadores de compromiso. Dependiendo de la severidad del ataque, existen varios métodos de recuperación, desde la reinstalación completa del sistema hasta la verificación manual de configuraciones actuales.

Este ataque destaca nuevamente la importancia de mantener actualizados los sistemas de gestión de seguridad y de aplicar las mejores prácticas de mitigación para reducir el riesgo de exposición ante vulnerabilidades críticas.

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-en-fortimanager-cibercriminales-aprovechan-fallo-de-autenticacion-para-ejecutar-codigo-remoto/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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/reporta-un-incidente