La seguridad de redes y servicios perimetrales es vital para proteger la confidencialidad, integridad y disponibilidad de la información corporativa. Este boletín presenta un análisis técnico de las vulnerabilidades publicadas por Fortinet considerando su impacto potencial sobre los sistemas en producción.

En abril de 2025, se descubrió una campaña de ciberataques a gran escala que ha comprometido más de 17,000 dispositivos Fortinet FortiGate a nivel mundial. La explotación de esta vulnerabilidad ha sido facilitada por fallas críticas previamente conocidas en dispositivos FortiGate, incluyendo CVE-2022-42475, CVE-2023-27997 y CVE-2024-21762. Aunque Fortinet ha lanzado actualizaciones para abordar estas vulnerabilidades, la persistencia del symlink malicioso (técnica empleada en la creación de un enlace simbólico) significa que los dispositivos pueden seguir comprometidos incluso después de aplicar los parches correspondientes.

Persistencia Post-Explotación en Dispositivos Fortinet: Técnicas Avanzadas de Enlace Simbólico:

En abril de 2025, se descubrió una campaña de ciberataques a gran escala que ha comprometido plataforma FortiGate Fortinet a nivel mundial:

- **Alcance del Ataque:** Más de 17,000 dispositivos Fortinet FortiGate en todo el mundo han sido comprometidos mediante una sofisticada técnica de persistencia que utiliza enlaces simbólicos (symlinks).
- **Método de Persistencia:** Los atacantes crearon un symlink que conecta el sistema de archivos del usuario con el sistema raíz en una carpeta utilizada para archivos de idioma del SSL-VPN. Esta modificación permite acceso de solo lectura a archivos sensibles y configuraciones, y persiste incluso después de actualizaciones de firmware estándar, ya que se realiza en una parte del sistema que no se sobrescribe durante dichas actualizaciones.

- **Vulnerabilidades Explotadas:** El ataque aprovecha vulnerabilidades conocidas previamente en dispositivos FortiGate, incluyendo fallas críticas documentadas en los últimos años.
- **Persistencia del Acceso:** Incluso después de aplicar parches para las vulnerabilidades originales, el symlink malicioso puede permanecer, proporcionando a los atacantes acceso persistente. El acceso de los atacantes podría incluir archivos de configuración sensibles, credenciales y claves criptográficas. En algunos casos, la intrusión podría haberse iniciado desde 2023, lo que sugiere que la campaña ha operado sin ser detectada durante un período significativo.

Impacto Global: Asia es la región más afectada, representando aproximadamente la mitad de los casos, seguida por Europa y América del Norte. América del Sur, África y Oceanía presentan números significativamente menores en comparación.

Indicadores de Compromiso:

Presencia de archivos sospechosos en el sistema. La existencia de estos artefactos en el sistema de archivos puede indicar una intrusión o manipulación maliciosa:

- /data/lib/libips.bak
- /data/lib/libgif.so
- /data/lib/libiptcp.so
- /data/lib/libipudp.so
- /data/lib/libjepg.so
- /var/.sslvpnconfigbk
- /data/etc/wxd.conf
- /flash

Conexiones salientes a direcciones IP maliciosas: Se ha identificado actividad de red anómala con intentos de conexión desde dispositivos FortiGate hacia las siguientes direcciones IP:

- 188.34.130.40:444
- 103.131.189.143:30080, 30081, 30443, 20443
- 193.36.119.61:8443, 444
- 172.247.168.153:8033
- 139.180.184.197

- 66.42.91.32
- 158.247.221.101
- 107.148.27.117
- 139.180.128.142
- 155.138.224.122
- 185.174.136.20

Recomendaciones:

Fortinet ha respondido a esta amenaza con actualizaciones de seguridad y recomendaciones específicas para mitigar el riesgo. Fortinet actuó rápidamente notificando a los clientes impactados y liberando actualizaciones específicas para diversas versiones de FortiOS.

Estas actualizaciones tienen como objetivo identificar y eliminar los enlaces simbólicos maliciosos, además de reforzar los sistemas contra técnicas similares de persistencia a futuro. Se recomienda a todos los usuarios migrar a las versiones corregidas: 7.6.2, 7.4.7, 7.2.11, 7.0.17 o 6.4.16.

No obstante, se advierte que instalar los parches no basta para erradicar el problema por completo. Se sugiere enfáticamente a la entidad:

- Actualizar los dispositivos FortiGate a versiones seguras (7.6.2, 7.4.7, 7.2.11, 7.0.17 o 6.4.16) según lo publicado por Fortinet, incluso si ya se aplicaron parches previos.
- Ejecutar escaneos en */data/lib*, */var* y otros directorios para detectar y eliminar symlinks maliciosos que persistan tras la actualización.
- Aislar equipos FortiGate potencialmente comprometidos en redes separadas, limitando su conectividad hasta descartar actividad maliciosa.
- Cambiar claves, tokens y certificados afectados, y activar alertas en el SIEM frente a IoCs e IPs maliciosas reportadas

Cabe señalar que los dispositivos que nunca activaron la funcionalidad SSL-VPN probablemente no están expuestos a esta amenaza particular.

Este ataque pone en evidencia una tendencia creciente entre los cibercriminales: explotar vulnerabilidades conocidas de manera ágil e integrar métodos de persistencia que sobreviven incluso a procesos normales de remediación. La posibilidad de que los atacantes mantengan

acceso luego de aplicar parches representa una amenaza considerable, especialmente en entornos con infraestructuras críticas.

Pasos para la actualización del Firmware:

1. Descargar el Firmware	Accede al portal de soporte de Fortinet (https://support.fortinet.com) y descarga la versión de firmware recomendada para tu modelo de dispositivo.
2. Respaldar la configuración	Antes de proceder, realizar una copia de seguridad de la configuración actual del dispositivo para prevenir pérdidas de datos en caso de fallos durante la actualización.
3. Proceso de actualización	1. Inicia sesión en la interfaz web del FortiGate como usuario administrador. 2. Navega a **System > Firmware & Registration**. 3. Selecciona tu dispositivo FortiGate y haz clic en **Upgrade**. 4. En la pestaña **File Upload**, haz clic en **Browse** y selecciona el archivo de firmware previamente descargado. 5. Haz clic en **Confirm and Backup Config** para iniciar el proceso de actualización. 6. El dispositivo respaldará la configuración actual, cargará la nueva imagen de firmware, realizará la actualización y se reiniciará automáticamente.
4. Verificación post-actualización	Una vez completada la actualización, verifica que el dispositivo esté funcionando correctamente y que la versión del firmware se haya actualizado según lo esperado.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

Fuentes:

- https://www.ecucert.gob.ec/wp-content/uploads/2025/04/Al-2025-016-Fortinet-FortiOS-y-FortiProxy.pdf
- https://cybersecuritynews.com/fortinet-devices-compromised/
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570