Boletín informativo
Vulnerabilidad Fortinet

CSIRTSALUD-AV-20251212-18 **TLP: CLEAR**

Incidente ID:	0018
Fecha del reporte:	12/12/2025
Entidad:	Ecosistema Digital
Título:	Vulnerabilidad Crítica Detectada en Fortinet
Herramienta de detección	N/A
Activo involucrado:	Herramientas Fortinet
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las Entidades del Ecosistema Digital sobre la vulnerabilidad crítica CVE-2025-64446, actualmente bajo explotación activa, que afecta a productos Fortinet, incluyendo FortiWeb, FortiOS y FortiProxy y que permite a actores maliciosos eludir los mecanismos de autenticación FortiCloud SSO, comprometer la integridad del dispositivo y obtener acceso no autorizado a la infraestructura protegida.

Descripción:

Se público una vulnerabilidad crítica CVE-2025-64446, la cual está siendo explotada activamente por Actores maliciosos, esta falla afecta a productos Fortinet, incluyendo FortiWeb, FortiOS y FortiProxy, y permite a un atacante eludir los mecanismos de autenticación FortiCloud SSO, acceder de forma no autorizada a la consola de administración y comprometer la integridad de los dispositivos afectados. Su impacto la clasifica como una vulnerabilidad de alta severidad, dado que posibilita el control completo del sistema sin necesidad de credenciales válidas.

La vulnerabilidad ha comenzado a ser explotada activamente en entornos reales, orientando ataques contra infraestructuras expuestas a Internet que utilizan FortiWeb y otros productos Fortinet vulnerables. La explotación permite a los atacantes obtener acceso administrativo, manipular configuraciones críticas y potencialmente desplegar payloads maliciosos dentro de la infraestructura afectada. Debido a la amplia adopción de estas soluciones perimetrales en Entidades públicas y privadas, podrían estar expuestas a compromisos significativos si no aplican las actualizaciones de seguridad correspondientes.

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

Productos afectados:

Las siguientes soluciones y versiones de productos Fortinet contienen la vulnerabilidad CVE-2025-64446.

Producto	Versiones vulnerables
FortiWeb	7.0.0 a 7.0.6, 7.2.0 a 7.2.4 a 8.0.0 – 8.0.1
FortiOS	7.4.0 a 7.4.2, 7.2.0 a 7.2.7
FortiProxy	7.0.0 a 7.0.13, 7.2.0 a 7.2.5

Modo de explotación

La vulnerabilidad CVE-2025-64446 permite a un atacante eludir el proceso de autenticación FortiCloud SSO en productos Fortinet (FortiWeb, FortiOS y FortiProxy), debido a una validación insuficiente de las firmas criptográficas utilizadas durante el flujo de inicio de sesión. Como resultado, un actor no autenticado puede obtener acceso administrativo a la interfaz de gestión del dispositivo.

Como se explota:

1. **Envío de una solicitud manipulada hacia el flujo de autenticación FortiCloud SSO**

El atacante envía una solicitud especialmente diseñada hacia el endpoint responsable del proceso de autenticación FortiCloud SSO.

La solicitud incluye un token SSO adulterado o una estructura de autenticación falsificada.
Este token debería ser verificado mediante una firma digital legítima, pero la vulnerabilidad permite que tokens modificados sean aceptados sin validación completa.

2. **Falla en la validación criptográfica del token**

El dispositivo Fortinet procesa el token SSO sin validar correctamente su firma, lo que impide verificar su autenticidad, detectar modificaciones o confirmar su origen confiable. Esta debilidad permite que un atacante inyecte un token manipulado que aparenta ser legítimo y que es aceptado por el sistema, habilitando el bypass del proceso de autenticación.

3. **Bypass de autenticación y elevación a sesión administrativa**

Una vez que el token fraudulento es aceptado, el sistema otorga acceso directo a la consola administrativa y genera una sesión como si el usuario hubiera completado un inicio de sesión legítimo, concediendo de inmediato

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

privilegios administrativos completos. Esto ocurre sin necesidad de contraseña, MFA ni credenciales válidas, lo que constituye un bypass total del mecanismo de autenticación.

4. **Acceso sin credenciales a la administración del dispositivo**

Con la sesión administrativa activa, el atacante puede modificar configuraciones del firewall, WAF o proxy, crear usuarios maliciosos, deshabilitar reglas de seguridad, desplegar configuraciones alteradas e incluso pivotar hacia otros segmentos de red internos. Este tipo de compromiso no requiere credenciales previas ni acceso interno, y puede ejecutarse de manera remota siempre que la interfaz de administración del dispositivo esté expuesta.

Recomendaciones de mitigación:

- Aplicar de inmediato las actualizaciones oficiales publicadas por Fortinet, instalando las versiones corregidas que eliminan la vulnerabilidad y reducen completamente el vector de explotación identificado.

  A continuación, se presentan las versiones vulnerables de Fortinet y su respectiva actualización para corregir la vulnerabilidad.

Producto Fortinet	Versiones vulnerables	Versiones corregidas
FortiWeb	7.0.0 – 7.0.6	7.0.12 o superior
	7.2.0 – 7.2.4	7.2.12 o superior
	7.4.0 – 7.4.2	7.4.10 o superior
	8.0.0 – 8.0.1	8.0.2 o superior
FortiOS	7.0.0 – 7.0.14	7.0.15 o superior
	7.2.0 – 7.2.7	7.2.8 o superior
	7.4.0 – 7.4.2	7.4.3 o superior
FortiProxy	7.0.0 – 7.0.13	7.0.14 o superior
	7.2.0 – 7.2.5	7.2.6 o superior

  Enlace de descarga oficial Fortinet:

  - https://support.fortinet.com/Download/FirmwareImages.aspx

- Bloquear acceso administrativo desde Internet; permitir solo desde IPs internas, bastion hosts o VPN.

- Si no es posible aplicar parches inmediatamente, deshabilitar FortiCloud SSO para evitar la ejecución del flujo vulnerable.

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

- Verificar accesos sospechosos, creación de cuentas, cambios no autorizados y sesiones abiertas antes del parcheo.
- Implementar autenticación multifactor para todas las cuentas administrativas, reduciendo riesgo de abuso de sesión.
- Deshabilitar servicios no utilizados, reforzar políticas de acceso, aplicar mínimo privilegio.
- Asegurar que las interfaces HTTP/HTTPS administrativas no estén expuestas a Internet sin controles estrictos.

Fuentes:

- https://fortiguard.fortinet.com/psirt/FG-IR-25-910?utm_source
- https://support.fortinet.com/Download/FirmwareImages.aspx
- https://cybersecuritynews.com/critical-fortinet-vulnerability/

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.

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