Boletín de alerta

Boletín Nro.:
Fecha de publicación: 10/12/2025
Tema: Alerta 2025-103 Vulnerabilidad Crítica en Productos Fortinet
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Esta vulnerabilidad impacta a múltiples soluciones de Fortinet relacionadas con seguridad de red, administración y protección web:

FortiOS

- 7.6.0 – 7.6.3
- 7.4.0 – 7.4.8
- 7.2.0 – 7.2.11
- 7.0.0 – 7.0.17

FortiProxy

- 7.6.0 – 7.6.3
- 7.4.0 – 7.4.10
- 7.2.0 – 7.2.14
- 7.0.0 – 7.0.21

FortiSwitchManager

- 7.2.0 – 7.2.6
- 7.0.0 – 7.0.5

FortiWeb

- 8.0.0
- 7.6.0 – 7.6.4
- 7.4.0 – 7.4.9

Descripción

Fortinet ha publicado un aviso crítico que afecta a FortiOS, FortiWeb, FortiProxy y FortiSwitchManager debido a un fallo en la verificación de firmas criptográficas dentro del proceso de autenticación de inicio de sesión único (SSO) basado en SAML. Esta debilidad permite que un atacante no autenticado cree un mensaje SAML falso y obtenga acceso administrativo sin autorización, incluso si no tiene credenciales válidas. Aunque el SSO de FortiCloud no está activado por defecto, muchos dispositivos quedan expuestos porque la opción se habilita automáticamente cuando se registran en FortiCare a través de la interfaz gráfica. Fortinet confirmó que la vulnerabilidad, descubierta por su propio equipo interno de seguridad, representa un riesgo grave para cualquier entorno donde el SSO esté habilitado, por lo que recomienda actualizar inmediatamente a las versiones corregidas.

La vulnerabilidad se basa en el proceso SAML, que funciona como un "pasaporte digital" usado para confirmar la identidad de un usuario; este pasaporte debería estar firmado criptográficamente por FortiCloud, pero los dispositivos afectados no verifican correctamente esa firma, lo que permite que un atacante genere un pasaporte falso (un mensaje SAML manipulado) que el dispositivo acepta como válido, otorgándole acceso administrativo sin necesidad de contraseña; en otras palabras, el atacante puede ingresar como administrador sin autenticarse realmente.

CVE-2025-59718

Afecta a FortiOS, FortiProxy y FortiSwitchManager. La vulnerabilidad permite que un atacante no autenticado evada la autenticación SSO de FortiCloud mediante un mensaje SAML manipulado cuya firma no es verificada correctamente. Esto puede resultar en acceso completo al dispositivo.

CVE-2025-59719

Afecta a FortiWeb. De forma similar, un mensaje SAML modificado puede ser aceptado por el dispositivo sin validar su firma, permitiendo la omisión del proceso de autenticación y acceso no autorizado al panel administrativo.

Solución:

Desactivar FortiCloud SSO temporalmente

Si está habilitado, apáguelo de inmediato. Esto bloquea el vector de ataque incluso sin aplicar parches.

Actualizar a versiones no afectadas (solución definitiva)

- FortiOS, versiones 7.6.4, 7.4.9, 7.2.12, 7.0.18 o superiores.
- FortiProxy, versiones 7.6.4, 7.4.11, 7.2.15, 7.0.22 o superiores.
- FortiSwitchManager, versiones 7.2.7, 7.0.6 o superiores.
- FortiWeb, versiones 8.0.1, 7.6.5, 7.4.10 o superiores.

https://docs.fortinet.com/upgrade-tool/fortigate

Información adicional:

https://fortiguard.fortinet.com/psirt/FG-IR-25-647

FortiOS, FortiWeb, and FortiProxy Vulnerability Lets Attackers Bypass FortiCloud SSO Authentication