Alerta

Técnica

Vulnerabilidades Críticas Detectadas en Fortinet

COLCERT AL – 20251217 - 089

TLP:CLEAR

Resumen Ejecutivo

Se ha identificado un conjunto de vulnerabilidades críticas que afectan dispositivos **Fortinet** ampliamente utilizados como componentes clave de seguridad perimetral. La explotación activa de estas fallas incrementa la probabilidad de accesos administrativos no autorizados en organizaciones que no han aplicado las actualizaciones de seguridad o mantienen configuraciones expuestas.

NIVEL DE RIESGO

ALTO

De continuar este escenario, existe un riesgo elevado de que estos accesos sean utilizados como habilitadores para ataques de mayor alcance, comprometiendo la confidencialidad, integridad y disponibilidad de servicios digitales críticos. En el contexto colombiano y regional, donde estos dispositivos tienen una alta adopción, la materialización de este riesgo podría generar impactos operativos y reputacionales significativos.

Vulnerabilidades identificadas

CVE	Producto afectado	Score CVSS	Descripción	CISA KEV
CVE-2025-59718	• FortiOS (versiones 7.0.0-7.0.17, 7.2.0-7.2.11, 7.4.0-7.4.8, 7.6.0-7.6.3) • FortiProxy (7.0.0-7.0.21, 7.2.0-7.2.14, 7.4.0-7.4.10, 7.6.0-7.6.3) • FortiSwitchManager (7.0.0-7.0.5, 7.2.0-7.2.6)	**9.8 (Crítico)**	Vulnerabilidad debido a verificación inadecuada de firmas criptográficas en el proceso de autenticación de **FortiCloud SSO**. Permite a un atacante no autenticado eludir la autenticación de inicio de sesión de **FortiCloud SSO** mediante un mensaje SAML manipulado, logrando así acceso administrativo sin credenciales válidas si la función **FortiCloud SSO** está habilitada.	**TRUE**
CVE-2025-59719	• FortiWeb (versiones 7.4.0-7.4.9, 7.6.0-7.6.4, 8.0.0)	**9.8 (Crítico)**	Similar a CVE-2025-59718, esta falla es una verificación incorrecta de firmas criptográficas en el proceso de autenticación **FortiCloud SSO** de **FortiWeb**. Permite a un atacante no autenticado evitar la autenticación mediante un mensaje SAML creado maliciosamente, resultando en acceso administrativo sin necesidad de credenciales cuando el **FortiCloud SSO** está activado.	**FALSE**

¿Qué indicó Fortinet al respecto?

Fortinet ha reconocido públicamente la existencia de las vulnerabilidades **CVE-2025-59718** y **CVE-2025-59719**, confirmando que afectan el mecanismo de autenticación asociado a **FortiCloud SSO** en varios de sus productos. La compañía informó que las fallas se originan por una validación insuficiente durante el proceso de autenticación y que, bajo ciertas condiciones de configuración, podrían permitir la omisión de los controles de inicio de sesión.

Fortinet publicó actualizaciones de seguridad para los productos afectados y advirtió que cuenta con **reportes de explotación activa en entornos reales**, motivo por el cual recomendó **aplicar los parches de manera inmediata** o, de forma temporal, deshabilitar el acceso administrativo mediante **FortiCloud SSO**. Asimismo, instó a los administradores a revisar registros de acceso y a reforzar las medidas de monitoreo ante posibles compromisos.

¿Cómo aprovechan los ciberdelincuentes estas vulnerabilidades?

1. **Uso indebido del mecanismo de autenticación SSO**: los productos afectados permiten el acceso administrativo mediante inicio de sesión centralizado (SSO), el cual confía en mensajes SAML enviados por un proveedor de identidad externo (FortiCloud). El problema radica en que el sistema vulnerable no valida correctamente la firma criptográfica de dichos mensajes SAML en determinados escenarios. Esto provoca que el dispositivo confíe en mensajes de autenticación que no han sido emitidos ni firmados legítimamente.

2. **Manipulación de mensajes de autenticación**: aprovechando esta debilidad, un ciberdelincuente remoto puede generar o modificar un mensaje SAML, incluir en ese mensaje atributos que simulan un usuario legítimo y omitir o alterar la firma criptográfica sin que el sistema lo detecte. Debido a la validación insuficiente, el dispositivo acepta el mensaje como válido y autoriza el acceso sin requerir credenciales reales.

3. **Omisión de la autenticación (Authentication Bypass)**: como resultado, el atacante logra acceso directo a la interfaz administrativa del dispositivo sin necesidad de conocer usuarios, contraseñas o certificados válidos desde la red o Internet, dependiendo de la exposición del servicio. Este comportamiento corresponde a una omisión completa de los controles de autenticación, clasificada como una vulnerabilidad crítica.

4. **Acciones posteriores al acceso no autorizado**: una vez obtenido el acceso administrativo, los atacantes suelen consultar o extraer archivos de configuración del dispositivo, analizar la topología de red, reglas de seguridad y políticas, preparar ataques posteriores contra otros sistemas conectados y mantener persistencia o facilitar accesos futuros. Este tipo de acceso representa un alto riesgo para la infraestructura, ya que compromete el control central del dispositivo de seguridad.

Impacto para Colombia y la región

- **Sectores afectados**: financiero, salud, TIC, gobierno, transporte, educación, energía y servicios públicos.
- **Riesgo alto**: el nivel de riesgo asociado a estas vulnerabilidades se considera alto para Colombia y la región debido a la amplia adopción de dispositivos Fortinet como elementos críticos de seguridad perimetral en infraestructuras públicas y privadas. La posibilidad de acceso administrativo sin autenticación válida, combinada con la explotación activa confirmada, incrementa significativamente la probabilidad de compromisos exitosos.
- **Posibles consecuencias**:
  - Compromiso de dispositivos de seguridad perimetral.
  - Exposición de configuraciones internas de red y políticas de seguridad.
  - Facilitación de ataques posteriores contra sistemas internos.
  - Interrupción de servicios digitales críticos.
  - Afectación a la continuidad operativa de organizaciones públicas y privadas.
- **Implicaciones en seguridad digital**: para Colombia y la región, este escenario refuerza la necesidad de fortalecer las prácticas de gestión de parches, monitoreo continuo de dispositivos de seguridad, revisión periódica de configuraciones y adopción de modelos de defensa en profundidad.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Exploit Public-Facing Application	**T1190**	Los ciberdelincuentes explotan una vulnerabilidad en una aplicación o servicio expuesto a Internet para obtener acceso inicial. En este caso, la explotación se realiza contra la interfaz administrativa web de dispositivos Fortinet accesibles desde la red.
Exploitation of Remote Services	**T1210**	El adversario aprovecha una falla en un servicio remoto para ejecutar acciones no autorizadas. Estas vulnerabilidades permiten abusar del servicio de autenticación remota basado en SAML para acceder al dispositivo sin credenciales válidas, obteniendo control administrativo del sistema.
Modify Authentication Process	**T1556**	El atacante abusa del proceso de autenticación para evadir los controles de acceso. En este escenario, se explota una validación incorrecta de firmas criptográficas en mensajes SAML, permitiendo que el sistema acepte autenticaciones forjadas como legítimas.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Update Software	**M1051**	Es la mitigación principal para este escenario, ya que las vulnerabilidades CVE-2025-59718 y CVE-2025-59719 se corrigen mediante actualizaciones oficiales de Fortinet.
Disable or Remove Feature or Program	**M1042**	Resulta altamente relevante, ya que Fortinet recomendó deshabilitar temporalmente el acceso administrativo mediante FortiCloud SSO cuando no sea estrictamente necesario. Al eliminar o desactivar esta funcionalidad vulnerable, se reduce de forma inmediata la superficie de ataque explotada por los adversarios.
Network Segmentation	**M1030**	Limitar el acceso a las interfaces administrativas de los dispositivos Fortinet mediante segmentación de red reduce significativamente el riesgo de explotación remota.

Soluciones y mitigaciones disponibles

✓ Actualizar los productos Fortinet afectados aplicando de manera inmediata las versiones de software publicadas por el fabricante que corrigen las fallas en el proceso de autenticación **FortiCloud SSO**:

Producto	Versión mínima segura a actualizar
FortiOS	7.0.18 / 7.2.12 / 7.4.9 / 7.6.4
FortiProxy	7.0.22 / 7.2.15 / 7.4.11 / 7.6.4
FortiSwitchManager	7.0.6 / 7.2.7
FortiWeb	8.0.1 / 7.6.5 / 7.4.10

✓ Deshabilitar el acceso administrativo mediante **FortiCloud SSO** en aquellos entornos donde no sea estrictamente necesario, como medida preventiva temporal o complementaria al parcheo, con el fin de reducir la superficie de ataque y evitar la explotación de la omisión de autenticación mientras se completan las tareas de actualización.

✓ Restringir el acceso a las interfaces administrativas de los dispositivos Fortinet limitándolo únicamente a redes internas o direcciones IP autorizadas, evitando la exposición directa de los servicios de gestión a Internet y disminuyendo la probabilidad de explotación remota de estas vulnerabilidades.

✓ Revisar de forma exhaustiva los registros de autenticación y administración para identificar accesos anómalos, sesiones SSO inesperadas o eventos administrativos desde direcciones IP no habituales, lo cual permite detectar posibles compromisos asociados a la explotación de estas fallas.

✓ Rotar las credenciales administrativas y revisar las cuentas existentes en los dispositivos afectados, especialmente en escenarios donde se sospeche o confirme explotación, con el objetivo de prevenir accesos persistentes y asegurar que no existan cuentas o configuraciones maliciosas creadas durante un acceso no autorizado.

Fuentes

FortiGuard Labs, 9 diciembre 2025, FG-IR-25-647 Multiple Fortinet Products' FortiCloud SSO Login Authentication Bypass, Fuente oficial del fabricante.
https://www.fortiguard.com/psirt/FG-IR-25-647
BleepingComputer.com, 16 diciembre 2025, Hackers exploit newly patched Fortinet auth bypass flaws, Fuente periodística técnica.
https://www.bleepingcomputer.com/news/security/hackers-exploit-newly-patched-fortinet-auth-bypass-flaws/
National Vulnerability Database (NVD), 9 diciembre 2025, consulta 16 diciembre 2025, CVE-2025-59718 Detail, Registro de vulnerabilidad oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-59718
National Vulnerability Database (NVD), 9 diciembre 2025, consulta 16 diciembre 2025, CVE-2025-59719 Detail, Registro de vulnerabilidad oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-59719