# Boletín de alerta

**Boletín Nro.:** 7
**Fecha de publicación:** 22/01/2026
**Tema:** Alerta 2026-07 Vulnerabilidad en el SSO de Fortinet explotada activamente
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

Las versiones de los siguientes productos están afectados:

- FortiOS:
  - De 7.6.0 a 7.6.3;
  - De 7.4.0 a 7.4.8;
  - De 7.2.0 a 7.2.11;
  - De 7.0.0 a 7.0.17.
- FortiProxy:
  - De 7.4.0 a 7.4.10;
  - De 7.2.0 a 7.2.14;
  - De 7.0.0 a 7.0.21.
- FortiSwitchManager:
  - De 7.2.0 a 7.2.6
  - De 7.0.0 a 7.0.5.
- FortiWeb:
  - 8.0.0;
  - De 7.6.0 a 7.6.4;
  - De 7.4.0 a 7.4.9.

Nota: Las versiones anteriores también pueden verse afectadas; consulte el aviso de Fortinet.

## Descripción

Se ha reportado una vulnerabilidad crítica en la función de inicio de sesión único (SSO) de Fortinet para firewalls FortiGate, identificada como CVE-2025-59718 , está bajo explotación activa. Actualmente tiene un score de CVSSv3 9.8 (Crítica).

- **CVE-2025-59718** : la vulnerabilidad afecta a las versiones de los productos FortiOS, FortiProxy y FortiSwitchManager ya mencionadas anteriormente.

- **CVE-2025-59719** : la vulnerabilidad afecta a las versiones del producto FortiWeb ya mencionadas anteriormente.

Los atacantes lo están aprovechando para crear cuentas de administrador locales no autorizadas, otorgando acceso administrativo completo a dispositivos expuestos a Internet.

La falla persiste a pesar de los parches, lo que permite la escalada de privilegios en firewalls que utilizan SAML o FortiCloud SSO para la autenticación de administrador.

## Mitigación

Deshabilite los inicios de sesión SSO de FortiCloud a través de CLI para bloquear la explotación:

```
config system global
set admin-forticloud-sso-login disable
end
```

Esto previene ataques basados en SSO sin interrumpir la autenticación local o SAML. Vuelva a habilitarlo después de la actualización. Fortinet recomienda su aplicación inmediata, especialmente en firewalls con acceso a internet.

- **Registros de auditoría** : revisión de inicios de sesión SSO sospechosos y nuevos administradores (por ejemplo, “servicio de asistencia técnica”).
- **Segmentación de red** : restrinja el acceso de administrador; aplique políticas de entrada local.
- **Monitoreo** : Integre SIEM para cambios administrativos; escanee en busca de IOC como IP/inicios de sesión coincidentes.
- **Aplicación de parches** : actualizar a versiones corregidas al momento del lanzamiento; probar en fase de prueba.
- **Respuesta empresarial** : en caso de riesgo, rote las credenciales, aísle los dispositivos y comuníquese con el soporte de Fortinet.

Fortinet promete avisos pronto. Este incidente pone de relieve los riesgos del SSO en los firewalls, la desactivación de funciones innecesarias y la monitorización intensiva. Estén atentos a CVSS y a los IOC completos.

## IoCs

| **IOC** | Tipo |
|---|---|
| cloud-init@mail[.]io | Cuenta maliciosa observada iniciando sesión en dispositivos de firewall, descargando/exfiltrando un archivo de configuración de firewall |
| cloud-noc@mail[.]io | Cuenta maliciosa observada iniciando sesión en dispositivos de firewall, descargando/exfiltrando un archivo de configuración de firewall |
| 104.28.244[.]115 | IP de origen observado en intrusiones |
| 104.28.212[.]114 | IP de origen observado en intrusiones |

| | |
|---|---|
| 217.119.139[.]50 | IP de origen observado en intrusiones |
| 37.1.209[.]19 | IP de origen observado en intrusiones |
| secadmin | Cuenta creada tras el acceso inicial |
| itadmin | Cuenta creada tras el acceso inicial |
| support | Cuenta creada tras el acceso inicial |
| backup | Cuenta creada tras el acceso inicial |
| remoteadmin | Cuenta creada tras el acceso inicial |
| audit | Cuenta creada tras el acceso inicial |

## Solución

El proveedor ha proveído parches de seguridad para las siguientes versiones:

| Versión | Afectado | Solución |
|---|---|---|
| **FortiOS 7.6** | 7.6.0 a 7.6.3 | Actualice a 7.6.4 o superior |
| **FortiOS 7.4** | 7.4.0 a 7.4.8 | Actualice a 7.4.9 o superior |
| **FortiOS 7.2** | 7.2.0 a 7.2.11 | Actualice a 7.2.12 o superior |
| **FortiOS 7.0** | 7.0.0 a 7.0.17 | Actualice a 7.0.18 o superior |
| **FortiOS 6.4** | No afectado | No aplicable |
| **FortiProxy 7.6** | 7.6.0 a 7.6.3 | Actualice a 7.6.4 o superior |
| **FortiProxy 7.4** | 7.4.0 a 7.4.10 | Actualice a 7.4.11 o superior |
| **FortiProxy 7.2** | 7.2.0 a 7.2.14 | Actualice a 7.2.15 o superior |
| **FortiProxy 7.0** | 7.0.0 a 7.0.21 | Actualice a 7.0.22 o superior |
| **Administrador de conmutadores Forti 7.2** | 7.2.0 a 7.2.6 | Actualice a 7.2.7 o superior |
| **Administrador de conmutadores Forti 7.0** | 7.0.0 a 7.0.5 | Actualice a 7.0.6 o superior |
| **FortiWeb 8.0** | 8.0.0 | Actualice a 8.0.1 o superior |
| **FortiWeb 7.6** | 7.6.0 a 7.6.4 | Actualice a 7.6.5 o superior |
| **FortiWeb 7.4** | 7.4.0 a 7.4.9 | Actualice a 7.4.10 o superior |
| **FortiWeb 7.2** | No afectado | No aplicable |
| **FortiWeb 7.0** | No afectado | No aplicable |

Sigue la herramienta de actualización proveída por el fabricante para más información de como actualizar sus dispositivos:

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

## Información adicional:

- https://cybersecuritynews.com/fortinet-sso-vulnerability-exploited/

- https://www.fortiguard.com/psirt/FG-IR-25-647
- https://nvd.nist.gov/vuln/detail/CVE-2025-59718