Boletín de alerta

Boletín Nro.:
Fecha de publicación: 02/03/2026
Tema: Alerta 2026-19 Riesgo Crítico en FortiOS, FortiManager y FortiAnalyzer
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

La vulnerabilidad **CVE-2026-24858** afecta a los siguientes productos **cuando FortiCloud Single Sign-On (SSO)** está habilitado:

- FortiOS versiones: 6.4, 7.0, 7.2, 7.4, 7.6, 8.0
- FortiManager versiones: 7.0, 7.2, 7.4, 7.6, 8.0
- FortiAnalyzer versiones: 6.4, 7.0, 7.2, 7.4, 7.6
- FortiProxy versiones: 7.0, 7.2, 7.4, 7.6
- FortiSwitchManager versiones: 7.0, 7.2
- FortiWeb versiones: 7.0, 7.2, 7.4, 7.6, 8.0

Descripción

Se ha reportado la **explotación activa** de la vulnerabilidad crítica Zero-Day **CVE-2026-24858 (**Identificado por Fortinet como FG-IR-26-060**) con CVSSv3 9.4**, la cual permite a un atacante omitir mecanismos de autenticación (CWE-288) cuando está habilitado **FortiCloud SSO**.

Un atacante que posea una cuenta maliciosa en FortiCloud podría autenticarse mediante SSO en dispositivos registrados en cuentas de terceros y obtener **acceso administrativo completo**.

Esto significa que un equipo podría ser comprometido totalmente, incluso si se encuentra actualizado frente a vulnerabilidades anteriores.

La vulnerabilidad solo puede explotarse cuando **FortiCloud SSO está habilitado**. Aunque esta función no está activa por defecto, suele habilitarse durante el registro de FortiCare si no se desactiva manualmente.

Fortinet deshabilitó temporalmente el servicio a nivel servidor como medida de contención, pero confirmó que el riesgo continúa para dispositivos vulnerables.

Mitigación

La autenticación SSO de FortiCloud ya no admite el inicio de sesión desde dispositivos que ejecutan versiones vulnerables. Por lo tanto, actualmente no es necesario deshabilitar el inicio de sesión SSO de FortiCloud en el cliente.

Como referencia, se puede hacer de la siguiente manera:
En FortiOS y FortiProxy:
vaya a Sistema -> Configuración -> Desactive «Permitir inicio de sesión administrativo con FortiCloud SSO». O escriba el siguiente comando en la línea de comandos de la CLI:

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

En FortiManager y FortiAnalyzer:
vaya a Configuración del sistema -> SSO SAML -> Desactive la opción «Permitir que los administradores inicien sesión con FortiCloud». O escriba el siguiente comando en la línea de comandos de la CLI:

```
config system saml
    set forticloud-sso disable
end
```

Indicadores de compromiso

Cuentas de usuario de inicio de sesión SSO

- **cloud-noc@mail.io**
- **cloud-init@mail.io**
- **heltaylor.12@tutamail.com**
- **soporte@openmail.pro**

Direcciones IP

- 104.28.244.115
- 104.28.212.114
- 104.28.212.115
- 104.28.195.105
- 104.28.195.106
- 104.28.227.106
- 104.28.227.105
- 104.28.244.114
- 163.61.198.15
- 104.28.195.106
- 104.28.244.116
- 38.54.6.28
- 37.1.209.19

- 217.119.139.50

Solución:

Actualizar a las versiones corregidas indicadas anteriormente

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

FortiAnalyzer

- **7.6.0 – 7.6.5 Actualizar a 7.6.6 o superior**
- **7.4.0 – 7.4.9 Actualizar a 7.4.10 o superior**
- **7.2.0 – 7.2.11 Actualizar a 7.2.12 o superior**
- **7.0.0 – 7.0.15 Actualizar a 7.0.16 o superior**
- **6.4 No afectado**

FortiManager

- **7.6.0 – 7.6.5 Actualizar a 7.6.6 o superior**
- **7.4.0 – 7.4.9 Actualizar a 7.4.10 o superior**
- **7.2.0 – 7.2.11 Actualizar a 7.2.13 o superior**
- **7.0.0 – 7.0.15 Actualizar a 7.0.16 o superior**
- **6.4 No afectado**

FortiOS

- **7.6.0 – 7.6.5 Actualizar a 7.6.6 o superior**
- **7.4.0 – 7.4.10 Actualizar a 7.4.11 o superior**
- **7.2.0 – 7.2.12 Actualizar a 7.2.13 o superior**
- **7.0.0 – 7.0.18 Actualizar a 7.0.19 o superior**
- **6.4 No afectado**

FortiProxy

- **7.6.0 – 7.6.4 Actualizar a 7.6.6 o superior**
- **7.4.0 – 7.4.12 Actualizar a 7.4.13 o superior**
- **7.2.x y 7.0.x Migrar a versión corregida**

Para información sobre el reporte de Fortinet puede ir al siguiente enlace
https://www.fortiguard.com/psirt/FG-IR-26-060

Información adicional:

- https://www.fortiguard.com/psirt/FG-IR-26-060
- https://docs.fortinet.com/upgrade-tool/fortigate