| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2026-005 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR | ecucert |
| TLP: | TLP:CLEAR | **Aviso de seguridad** | |
| Fecha: | 02-feb-2026 | **Productos Fortinet FortiCloud SSO** | V 1.1 |

## I. DATOS GENERALES:

**Clase de alerta:** Bypass de autenticación.

**Tipo de incidente:** Fallo de Autenticación.

**Nivel de riesgo:** Alto

## II. INTRODUCCIÓN

- Una vulnerabilidad de verificación incorrecta de la firma criptográfica [CWE-347] en FortiOS, FortiWeb, FortiProxy y FortiSwitchManager puede permitir que un atacante no autenticado evite la autenticación de inicio de sesión SSO de FortiCloud a través de un mensaje SAML diseñado, si esa función está habilitada en el dispositivo.

## III. VECTOR DE ATAQUE:

Fortinet ha confirmado una vulnerabilidad crítica de bypass de autenticación en la funcionalidad FortiCloud SSO, activamente explotada bajo el identificador CVE-2026-24858. Esta falla afecta a varios productos incluyendo FortiOS, FortiManager, FortiAnalyzer y FortiProxy, y permite que un atacante con cuenta FortiCloud y dispositivo registrado acceda a otros dispositivos asociados a cuentas diferentes si FortiCloud SSO está habilitado, afectando la confidencialidad, integridad y disponibilidad del sistema.

El CVE-2026-24858 es una vulnerabilidad de bypass de autenticación (SSO) en múltiples productos de Fortinet. Un atacante remoto sin credenciales puede evadir el inicio de sesión de administrador en dispositivos Fortinet aprovechando el mecanismo de Single Sign-On (SSO) de FortiCloud. En concreto, un usuario malicioso con su propia cuenta de FortiCloud (y al menos un dispositivo Fortinet registrado en ella) puede autenticarse como administrador en dispositivos de otros usuarios si estos tienen habilitada la función de SSO con FortiCloud. Esto ocurre debido a un fallo en el proceso de SSO que permite una ruta alternativa de autenticación, posibilitando el acceso no autorizado.

CVE-2026-24858 tiene una puntuación **CVSSv3 de 9.4 (crítica),** permite el control de acceso inapropiado en el componente GUI (CWE-288). Se ha reportado explotación activa con acceso sin privilegios, sin interacción del usuario requerida y afectando sistemas remotos.



Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

| Nro. Alerta: | AL-2026-005 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR | |
|---|---|---|---|
| TLP: | TLP:CLEAR | **Aviso de seguridad** | ecucert |
| Fecha: | 02-feb-2026 | **Productos Fortinet FortiCloud SSO** | V 1.1 |

## IV. INDICADORES DE COMPROMISO:

- Entradas inusuales de autenticación FortiCloud desde cuentas o dispositivos que no corresponden con la organización objetivo.
- Eventos de creación de cuentas administrativas locales no autorizadas en dispositivos FortiOS, FortiManager o FortiAnalyzer.
- Descargas de configuraciones completas de dispositivos fuera de los horarios normales de administración.
- Alertas en logs de autenticación que muestren login exitoso a múltiples dispositivos desde una misma identidad FortiCloud. Cambios de políticas de red (firewall, VPN, ACL) que no se correlacionen con actividad de administradores legítimos.

**Recursos Afectados**

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.

## V. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:



Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

| Nro. Alerta: | AL-2026-005 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR | |
|---|---|---|---|
| TLP: | TLP:CLEAR | **Aviso de seguridad** | ecucert |
| Fecha: | 02-feb-2026 | **Productos Fortinet FortiCloud SSO** | V 1.1 |

- Actualizar inmediatamente todos los dispositivos afectados a versiones parcheadas:
- FortiOS: 7.6.6+, 7.4.11+, 7.2.13+, 7.0.19+
- FortiManager: 7.6.6+, 7.4.10+, 7.2.13+, 7.0.16+
- FortiAnalyzer: 7.6.6+, 7.4.10+, 7.2.12+, 7.0.16+
- FortiProxy: versiones actualizadas disponibles según rama de producto.
- Deshabilitar FortiCloud SSO temporalmente si no es indispensable, para reducir vectores de ataque hasta que se apliquen parches.

Revisar y auditar configuraciones y accesos tras aplicar parches para asegurar que no existan cuentas administrativas maliciosas o cambios indeseados.
Monitorear logs de autenticación FortiCloud y alertar sobre patrones sospechosos de acceso entre dispositivos vinculados a distintas cuentas.

Tenga en cuenta que la función de inicio de sesión SSO de FortiCloud no está habilitada en la configuración predeterminada de fábrica. Sin embargo, cuando un administrador registra el dispositivo en FortiCare desde la interfaz gráfica de usuario (GUI), a menos que desactive la opción "Permitir inicio de sesión administrativo con FortiCloud SSO" en la página de registro, el inicio de sesión SSO de FortiCloud se habilita al registrarse.

Para evitar verse afectado por esta vulnerabilidad en versiones vulnerables, desactive temporalmente la función de inicio de sesión de FortiCloud (si está habilitada) hasta actualizar a una versión no afectada.

Para desactivar el inicio de sesión de FortiCloud, vaya a Sistema -> Configuración ->

Desactive la opción "Permitir inicio de sesión administrativo mediante SSO de FortiCloud". O escriba el siguiente comando en la CLI: configuración del sistema global establecer admin-forticloud-sso-login deshabilitar.

## VI. REFERENCIAS:


- CERT-RAD-AS-21-2026_260129_092825.pdf
- https://www-fortiguard-com.translate.goog/psirt/FG-IR-25-647?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc




Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

| Nro. Alerta: | AL-2026-005 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR | |
|---|---|---|---|
| TLP: | TLP:CLEAR | **Aviso de seguridad** | ecucert |
| Fecha: | 02-feb-2026 | **Productos Fortinet FortiCloud SSO** | V 1.1 |

- https://unaaldia.hispasec.com/2026/02/vulnerabilidad-critica-de-bypass-de-autenticacion-en-fortinet-forticloud-sso.html
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/omision-de-autenticacion-en-el-inicio-de-sesion-sso-en-productos-de-fortinet
- https://nvd.nist.gov/vuln/detail/CVE-2026-24858



Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec