Boletín de alerta

Boletín Nro.:
Fecha de publicación: 29/01/2026
Tema: Alerta 2026-10 Vulnerabilidad Critica Fortinet
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- FortiManager 7.6.0 – 7.6.5, 7.2.0 – 7.2.11, 7.4.0 – 7.4.9, 7.6.0 – 7.6.5
- FortiOS 7.0.0 – 7.0.18, 7.2.0 – 7.2.12, 7.4.0 – 7.4.10, 7.6.0 – 7.6.5
- FortiAnalyzer 7.0.0 – 7.0.15, 7.2.0 – 7.2.11, 7.4.0 – 7.4.9, 7.6.0 – 7.6.5
- FortiProxy 7.0, 7.2, 7.4.0 – 7.4.12, 7.6.0 – 7.6.4
- FortiWeb 7.4.0 – 7.4.11, 7.6.0 – 7.6.6, 8.0.0 – 8.0.3

Descripción

Una vulnerabilidad de omisión de autenticación mediante una ruta o canal alternativo [CWE-288] en FortiOS, FortiManager, FortiAnalyzer, FortiProxy y FortiWeb podría permitir que un atacante con una cuenta de FortiCloud y un dispositivo registrado inicie sesión en otros dispositivos registrados en otras cuentas, si la autenticación SSO de FortiCloud está habilitada en dichos dispositivos. Se etiqueto como CVE-2026-24858 con CVSSv3 9.4.

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) del dispositivo, a menos que desactive la opción «Permitir inicio de sesión administrativo mediante SSO de FortiCloud» en la página de registro, el inicio de sesión SSO de FortiCloud se habilita al registrarse.

Ya se han reportado casos de explotación de esta vulnerabilidad, lo que lo hace más urgente. FortiManager Cloud, FortiAnalyzer Cloud y FortiGate Cloud no se ven afectados.

Solución

Los clientes deben actualizar a las últimas versiones del software para que funcione la autenticación SSO de FortiCloud

Información adicional:

- https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html
- https://www.cisa.gov/news-events/alerts/2026/01/28/fortinet-releases-guidance-address-ongoing-exploitation-authentication-bypass-vulnerability-cve-2026
- https://cyberpress.org/fortinet-actively-exploited-forticloud-sso-vulnerability-cve-2026-24858/
- https://arcticwolf.com/resources/blog/cve-2026-24858/