Boletín informativo vulnerabilidad FortiOS SSL VPN

CSIRTSALUD-AV-20251226-21 **TLP: CLEAR**

Incidente ID:	0021
Fecha del reporte:	26/12/2025
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad FortiOS SSL VPN
Herramienta de detección	N/A
Activo involucrado:	Firewall Fortinet
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre la explotación de la vulnerabilidad con código **CVE-2020-12812**, esta vulnerabilidad de nivel crítica **(CVSS 9.8)** de Fortinet FortiGate que fue parcheada hace tiempo, desde julio de 2020, está siendo explotada activamente eludiendo la autenticación de dos factores (2FA) en firewalls y potencialmente concediendo acceso no autorizado a VPNs y consolas de administración.

Descripción:

Los ciberdelincuentes están abusando activamente de una falla de Fortinet FortiGate, parcheada hace tiempo desde julio de 2020, eludiendo la autenticación de dos factores (2FA)

en los firewalls y potencialmente otorgando acceso no autorizado a VPN y consolas de administración.

El problema, denominado **FG-IR-19-283 (CVE-2020-12812)**, se debe a una discrepancia en la forma en que los dispositivos FortiGate gestionan los nombres de usuario en comparación con los directorios LDAP. FortiGate distingue entre mayúsculas y minúsculas por defecto, mientras que la mayoría de los servidores LDAP, como Active Directory, no distinguen entre mayúsculas y minúsculas.

Los atacantes explotan esto en configuraciones incorrectas donde los usuarios locales de FortiGate tienen activado el 2FA y también son miembros de grupos LDAP asignados a políticas de autenticación. El ataque se desarrolla de forma sencilla.

La vulnerabilidad ha sido explotada activamente por múltiples actores de amenazas , y el gobierno de EE. UU. también la incluye entre las muchas debilidades que se utilizaron como arma en ataques dirigidos a dispositivos de tipo perimetral en 2021.

Productos afectados:

La vulnerabilidad reside específicamente en el sistema operativo FortiOS.

Las versiones afectadas son:

Producto	Versiones Afectadas
FortiOS	Versión 6.4.0
FortiOS	Versiones 6.2.0 a 6.2.3
FortiOS	Versiones 6.0.9 y anteriores

Como se podría explotar esta vulnerabilidad

Para que se pueda explotar la vulnerabilidad se debe cumplir previamente los siguientes requisitos

- Entradas de usuarios locales en FortiGate con 2FA, con referencia a LDAP
- Los mismos usuarios deben ser miembros de un grupo en el servidor LDAP
- Al menos un grupo LDAP del que son miembros los usuarios de dos factores debe estar configurado en FortiGate, y el grupo debe usarse en una política de autenticación que podría incluir, por ejemplo, usuarios administrativos, SSL o VPN IPSEC.

La falla ocurre en el proceso de autenticación de la VPN SSL. Un atacante puede eludir el requisito de **FortiToken** o cualquier otro método de 2FA si logra lo siguiente:

- El atacante utiliza credenciales válidas (previamente obtenidas por phishing o fuerza bruta).

- Al enviar la solicitud de autenticación, el atacante altera el caso (mayúsculas/minúsculas) del nombre de usuario en una etapa específica del protocolo, o aprovecha que el sistema no exige el segundo factor si el usuario logra autenticarse contra un servidor LDAP/RADIUS externo que el FortiGate no valida correctamente para el paso de 2FA.

- El sistema otorga acceso completo a la red corporativa como si el usuario hubiera ingresado el código OTP.

Los atacantes suelen utilizar esta vulnerabilidad dentro de las siguientes técnicas de a taque (MITRE ATT&CK):

- **T1078 - Valid Accounts:** Uso de cuentas legítimas para infiltrarse.

- **T1556.006 - Modify Authentication Process:** Evasión de mecanismos de autenticación multifactor (MFA).
- **T1133 - External Remote Services:** Aprovechamiento de gateways VPN para obtener acceso inicial.

Indicadores de Compromiso (IoCs)

Para detectar si esta vulnerabilidad ha sido explotada en su entorno, revise los logs de su dispositivo FortiGate buscando:

- **Logs de Eventos VPN:** Entradas donde un usuario inicia sesión exitosamente en la VPN SSL sin que aparezca el registro correspondiente a la validación del token (OTP).
- **Anomalías en el Usuario:** Inicios de sesión con variaciones extrañas en el uso de mayúsculas (ej. Admin vs admin) que no coinciden con la base de datos de usuarios estándar.
- **IPs Inusuales:** Conexiones exitosas desde geografías no habituales o direcciones IP asociadas con nodos de salida TOR y proxies conocidos.

Recomendaciones de mitigación:

- Fortinet ha lanzado parches oficiales para corregir este comportamiento. La recomendación inmediata es **actualizar el firmware** a las versiones que contienen el parche de seguridad:

➢ **6.4.x:** Actualizar a **FortiOS 6.4.1** o superior.
➢ **6.2.x:** Actualizar a **FortiOS 6.2.4** o superior.
➢ **6.0.x:** Actualizar a **FortiOS 6.0.10** o superior.

- Desactivar la Sensibilidad a Mayúsculas y Minúsculas: En sistemas no parcheados, ejecutar set username-case-sensitivity disable (FortiOS 6.0.10–6.0.12, etc.) o set username-sensitivity disable (v6.0.13+, v6.2.10+, v6.4.7+, v7.0.1+).

- Recortar Grupos LDAP: Eliminar grupos secundarios innecesarios de las políticas. Sin ellos, los inicios de sesión no coincidentes fallan directamente.

Fuentes:

- https://cybersecuritynews.com/fortigate-firewall-vulnerability/
- https://thehackernews.com/search/label/Vulnerability

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.