| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2024-003 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert<br>V 1.1 |
| TLP: | TLP:CLEAR | | |
| Fecha: | 14-feb-2024 | **Vulnerabilidades de ejecución remota de código en FortiOS SSL VPN** | Pág.: **1** of **7** |

## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad

**Tipo de incidente:** Vulnerabilidad de ejecución remota de código en FortiOS SSL VPN, permite a atacantes no autenticados obtener ejecución remota de código a través de métodos maliciosos como COATHANGER.

**Nivel de riesgo:** Alto

## II. ALERTA

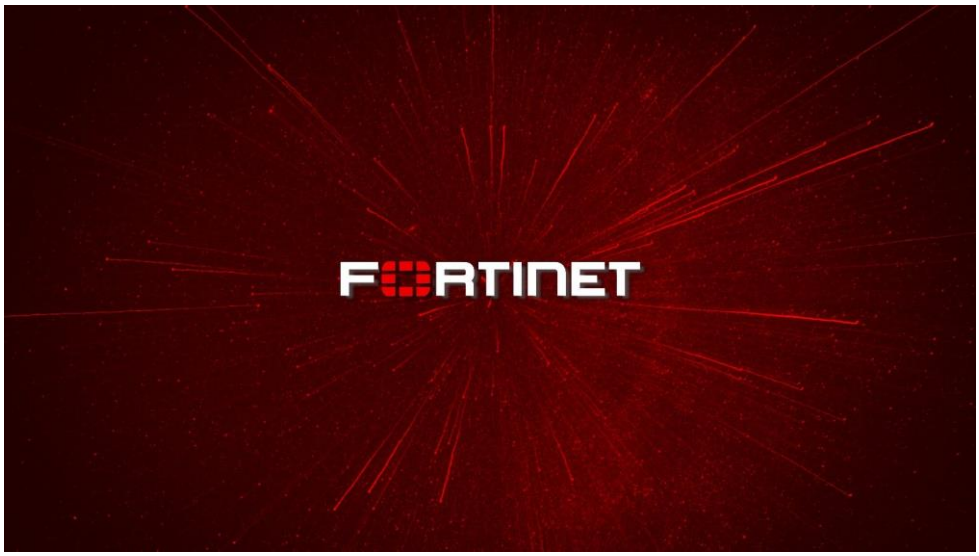


**Figura 1.-** ***Fallo crítico de RCE***

## III. INTRODUCCIÓN

Se han descubierto vulnerabilidades de ejecución remota de código en FortiOS SSL VPN llamada (CVE-2024-21762 / FG-IR-24-015).

El problema se relaciona con un fallo de escritura fuera de límites en FortiOS SSL VPN, en algunas de sus versiones.

Al afectar a versiones de FortiOS 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15 y todas las versiones de FortiOS 6.0. Podría verse comprometido por un troyano de acceso remoto (RAT) el cual se denomina COATHANGER

FortiOS SSL VPN es una solución de red privada virtual (VPN) proporcionada por Fortinet a través de su sistema operativo FortiOS. Permite a los usuarios acceder de forma segura a la red corporativa a través de una conexión encriptada utilizando el protocolo SSL/TLS. Esta tecnología facilita la conexión remota a la red empresarial, brindando seguridad y protección de datos durante la transmisión.

FortiOS SSL VPN es parte del sistema operativo FortiOS desarrollado por Fortinet. Es una empresa privada que se especializa en soluciones de seguridad de red, este no proporciona su software como código abierto. Fortinet se fundó en el año 2000, y a lo largo de los años ha desarrollado y mejorado sus productos para abordar las necesidades de seguridad en redes empresariales.

Fortinet es responsable del desarrollo, mantenimiento y soporte de FortiOS y sus componentes, incluido FortiOS SSL VPN. El costo de utilizar FortiOs y sus funciones, incluyendo SSL VPN, generalmente implica licencias y suscripciones. Los detalles específicos sobre precios pueden variar según la necesidad de la empresa, el tamaño de la implementación y otros factores.

Se encontró una vulnerabilidad potencial de secuencias de escritura fuera de límites, en FortiOS SSL VPN.

## IV. VECTOR DE ATAQUE:

- Red.
- Ejecución remota de código (RCE) mediante solicitudes http maliciosamente elaboradas.

## V. IMPACTO:

Las fallas de Fortinet (muchas veces de día cero) comúnmente tienen como objetivo violar las redes corporativas en campañas de ciber espionaje y ataques de ransomware.

Dado que los atacantes remotos no autenticados pueden utilizar estas vulnerabilidades para ejecutar código arbitrario en dispositivos vulnerables, se recomienda encarecidamente proteger todos los dispositivos Fortinet lo antes posible.

Una escritura fuera de límites en Fortinet FortiOS versiones 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15 , 6.0.0 a 6.0.17, versiones de FortiProxy 7.4.0 a 7.4.2, 7.2.0 a 7.2.8, 7.0.0 a 7.0.14, 2.0.0 a 2.0.13, 1.2.0 a 1.2.13 , 1.1.0 a 1.1.6, 1.0.0 a 1.0.7 permite al atacante ejecutar código o comandos no autorizados a través de solicitudes específicamente diseñadas

CISA ordenó a las agencias federales de EE. UU. que protejan los dispositivos FortiOS y FortiProxy contra este error de seguridad en un plazo de siete días, antes del 16 de febrero, como lo exige la directiva operativa vinculante (BOD 22-01) emitida en noviembre de 2021.

Coathanger es un troyano de acceso remoto (RAT) que apunta a los dispositivos de seguridad de red Fortigate y recientemente se utilizó para abrir una puerta trasera a una red militar del Ministerio de Defensa holandés.

## VI. INDICADORES DE COMPROMISO

- **CVE-2024-21762**

CVSS scores for CVE-2024-21762

| Base Score | Base Severity | CVSS Vector | Exploitability Score | Impact Score | Source |
|---|---|---|---|---|---|
| 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 3.9 | 5.9 | nvd@nist.gov |
| Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None | Scope: Unchanged | Confidentiality: High | Integrity: High | Availability: High |
| 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H | 3.9 | 5.9 | psirt@fortinet.com |
| Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None | Scope: Unchanged | Confidentiality: High | Integrity: High | Availability: High |

- **CVE-2023-44487**

CVSS scores for CVE-2023-44487

| Base Score | Base Severity | CVSS Vector | Exploitability Score | Impact Score | Source |
|---|---|---|---|---|---|
| 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 3.9 | 3.6 | nvd@nist.gov |
| Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None | Scope: Unchanged | Confidentiality: None | Integrity: None | Availability: High |
| 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H | 0.0 | 0.0 | RedHat-CVE-2023-44487 |
| Attack Vector: Network | Attack Complexity: Low | Privileges Required: None | User Interaction: None | Scope: Unchanged | Confidentiality: None | Integrity: None | Availability: High |

## VII. RECOMENDACIONES:

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

- Los usuarios deben actualizar a la versión superiores que no sean estas: FortiOS 7.4.0 a 7.4.2, 7.2.0 a 7.2.6, 7.0.0 a 7.0.13, 6.4.0 a 6.4.14, 6.2.0 a 6.2.15 y todas las versiones de FortiOS 6.0. Esta actualización se puede realizar en la interfaz web.

  Consulte: *https://www.fortiguard.com/psirt/FG-IR-24-015*

- Para los usuarios que no puedan aplicar parches, se recomienda desactivar SSL VPN en sus dispositivos para mitigar las vulnerabilidades.

En general se debe considerar las siguientes recomendaciones:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Tener actualizado y utilizar, un software anti-virus

- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución.

- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.

- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001/27002 en su control "Concienciación con educación y capacitación en seguridad de la información" o "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas

- Implementar un plan de respuesta a emergencias de la Organización/Institución.

- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. REFERENCIAS:

- **Linked in (2024).***Alerta de Seguridad por Nuevas Vulnerabilidades (RCE) en Fortinet SSL VPN-Existe sospecha de explotación Activa – CVE-2024-21762 CVE-2024-23113.* *https://es.linkedin.com/pulse/alerta-de-seguridad-por-nuevas-vulnerabilidades-rce-en-fortinet-k3oze?trk=article-ssr-frontend-pulse_more-articles_related-content-card*

- **Bleepingcomputer (2024)**.*New Fortinet RCE flaw in SSL VPN likely exploited in attacks* *https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/*

- **CVEdetails (2024).** *Vulnerability Details: CVE-2023-44487.* *https://www.cvedetails.com/cve/CVE-2023-44487/?q=CVE-2023-44487+*

- **CVEdetails (2024)**. *Vulnerability Details: CVE-2024-21762.* *https://www.cvedetails.com/cve/CVE-2024-21762/?q=CVE-2024-21762*