BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Ransomware FunkSec impulsado por IA ataca a 85 víctimas con doble extorsión

TLP: CLEAR

17.01.2025

CLICK PARA EMPEZAR

En esta edición: ⟶ Botnets Ransomware FunkSec impulsado por IA ataca a 85 víctimas con doble extorsión

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones

NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Cisco Common Services Platform Collector Cross-Site Scripting Vulnerabilities

CVE-2025-0242

Medium (5.4)

Impacto: Ejecución código o comandos no autorizados.

Resumen: Múltiples vulnerabilidades en la interfaz de administración basada en web de Cisco Common Services Platform Collector (CSPC) podrían permitir a un atacante remoto autenticado llevar a cabo ataques de cross-site scripting (XSS) contra un usuario de dicha interfaz. Un atacante podría explotar estas vulnerabilidades inyectando código malicioso en páginas específicas de la interfaz.

Versiones Afectadas

- Estas vulnerabilidades afectan a Cisco CSPC, independientemente de la configuración del dispositivo.

Solución: Cisco ha publicado actualizaciones de software gratuitas que solucionan la vulnerabilidad descrita en este aviso.
Ver +INFO.

Fecha de Publicación: 08/ENE/2025 +INFO

Vulnerabilidad de severidad alta en Google Chrome

CVE-2025-0242

High (8.3)

Impacto: Ejecución código o comandos no autorizados.

Resumen: Type Confusion en V8 en Google Chrome podría permitir a un atacante remoto ejecutar código arbitrario dentro de un sandbox a través de una página HTML diseñada específicamente.

Versiones Afectadas

- Versiones anteriores a 131.0.6778.264/.265 para Windows y Mac
- Versiones anteriores 131.0.6778.264 para Linux

Solución: Se recomienda a los usuarios actualizar de inmediato sus navegadores Chrome a la versión más reciente: 131.0.6778.264 para Linux y 131.0.6778.264/.265 para Windows y Mac. Ver +INFO.

Fecha de Publicación: 07/ENE/2025 +INFO

SonicOS SSLVPN Authentication Bypass Vulnerability

CVE-2024-53704

Critical (8.2)

Impacto: Acceso no autorizado.

Resumen: Esta vulnerabilidad podría permitir a un actor malicioso evadir el proceso de autenticación del sistema SSLVPN, comprometiendo la seguridad de la red.

Versiones Afectadas

Para ver los equipos y las versiones afectadas, consulte + INFO.

Solución: Instale el parche más reciente lo antes posible en los productos afectados. Las últimas versiones están disponibles para su descarga en mysonicwall.com.

Fecha de Publicación: 07/ENE/2025 INFO

Multiple Vulnerabilities in Expedition Migration Tool Lead to Exposure of Firewall Credentials

CVE-2025-0103,CVE-2025-0104,CVE-2025-0105,CVE-2025-0106,CVE-2025-0107

High (7.8)

Impacto: Acceso no autorizado.

Resumen: Varias vulnerabilidades en la herramienta Expedition de Palo Alto Networks permiten a atacantes acceder a la base de datos, leer o manipular archivos, incluyendo credenciales en texto claro, configuraciones y claves API de dispositivos con PAN-OS..

Versiones Afectadas

- Expedición1 through < 1.2.101

Para más información, consulte + INFO.

Solución: Palo Alto Networks informó que las versiones 1.2.101 y superiores de Expedition no están afectadas por la vulnerabilidad. Ver +INFO.

Fecha de Publicación: 07/ENE/2025 INFO

Authentication bypass in Node.js websocket module

CVE-2024-55591

Critical (9.6)

Impacto: Ejecutar código o comandos no autorizados.

Resumen: Una vulnerabilidad de authentication bypass mediante un camino o canal alternativo [CWE-288] que afecta a FortiOS y FortiProxy podría permitir que un atacante remoto obtenga privilegios de super-administrador a través de solicitudes manipuladas al módulo websocket de Node.js.

Versiones Afectadas

- FortiOS - 7.0.0 through 7.0.16
- FortiProxy - 7.2.0 through 7.2.12
- FortiProxy - 7.0.0 through 7.0.19

Para más información, consulte + INFO.

Solución: Fortinet ha publicado actualizaciones de software que solucionan esta vulnerabilidad. Ver +INFO

Fecha de Publicación: 14/ENE/2025 +INFO

Hardcoded Session Secret Leading to Unauthenticated Remote Code Execution

CVE-2023-37936

Critical (9.6)

Impacto: Ejecutar código o comandos no autorizados.

Resumen: Una vulnerabilidad de uso de clave criptográfica codificada [CWE-321] en FortiSwitch podría permitir a un atacante remoto no autenticado, que posea la clave, ejecutar código no autorizado mediante solicitudes criptográficas especialmente diseñadas.

Versiones Afectadas

- FortiSwitch 7.4.0
- FortiSwitch 7.2 7.2.0 through 7.2.5

Para más información, consulte + INFO.

Solución: Fortinet ha publicado actualizaciones de software que solucionan esta vulnerabilidad. Ver +INFO

Fecha de Publicación: 14/ENE/2025 +INFO

Actualizaciones de seguridad del mes de Enero para productos Microsoft

Las actualizaciones de seguridad de Microsoft de enero de 2025 corrigieron 161 vulnerabilidades en diversos productos como Windows, Office, Hyper-V, BitLocker, Servicios de Escritorio Remoto y otros. De estas,3 fueron críticas, 97 importantes, 58 moderadas y 1 de baja severidad. Tres vulnerabilidades en particular se explotan activamente, permitiendo a los atacantes ejecutar código con privilegios elevados en Hyper-V y ejecutar código remoto sin necesidad de autenticación, afectando componentes como los Servicios de Escritorio Remoto.

Recomendación:

Es crucial que los usuarios y administradores de sistemas apliquen de inmediato las actualizaciones de seguridad de Microsoft de enero de 2025, ya que abordan varios problemas críticos que representan riesgos significativos de explotación.

Versiones Afectadas

A continuación, se presenta algunas de las vulnerabilidades:

- Versiones anteriores a Microsoft .NET Framework 4.6/4.6.2
- Versiones anteriores Windows Server 2016

Para más información Ver +INFO.

Fecha de Publicación: 16/ENE/2025 INFO

Security updates available for Mozilla Firefox y Thunderbird

CVE-2025-0245, CVE-2025-0247, CVE-2025-0244

Mozilla ha lanzado actualizaciones de seguridad para sus productos Firefox y Thunderbird, corrigiendo vulnerabilidades críticas que podrían permitir la ejecución de código arbitrario. Estas fallas podrían ser aprovechadas por un atacante para ejecutar código malicioso, obtener control total sobre el dispositivo y comprometer su seguridad.

Recomendación:

Para remediar la vulnerabilidad, se recomienda aplicar las actualizaciones y parches de seguridad disponibles en la página oficial del fabricante. Para más detalles, consulte directamente el sitio web. *Ver +INFO*

Versiones Afectadas

- Mozilla Firefox, en versiones anteriores a 134
- Mozilla Firefox ESR, en versiones anteriores a 128.6
- Mozilla Thunderbird, en versiones anteriores a 134
- Mozilla Thunderbird ESR, en versiones anteriores a 128.6

Fecha de Publicación: 08/ENE/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	FABRICANTE	CVE / ACCESO	CVSSV3	DESCRIPCIÓN
10/01/2025	Fortinet	CVE-2022-45856	4.6	Una vulnerabilidad de validación de certificado incorrecta [CWE-295] en las funciones SAML SSO de FortiClientWindows, FortiClientMac, FortiClientLinux, FortiClientAndroid y FortiClientiOS puede permitir a un atacante no autenticado interponerse en la comunicación entre FortiClient y el proveedor de servicios y el proveedor de identidad.
7/01/2025	PaloAlto Networks	CVE-2025-0104	4.7	Esta vulnerabilidad reflejada de secuencias de comandos entre sitios (XSS) en Palo Alto Networks Expedition permitiría a los atacantes ejecutar código JavaScript malicioso en el contexto del navegador de un usuario autenticado de Expedition si ese usuario autenticado hace clic en un enlace malicioso que permite ataques de phishing y podría provocar el robo de la sesión del navegador de Expedition
14/01/2024	Fortinet	CVE-2024-48886 CVE-2024-50563	8.0	Una vulnerabilidad de autenticación débil [CWE 1390] de la misma naturaleza en el demonio csfd de FortiManager podría permitir que un atacante no autenticado con acceso a la interfaz y puerto de Security Fabric eluda el proceso de autenticación y acceda a una lista restringida de características.
14/01/2024	Fortinet	CVE-2023-37937	7.6	Una neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo [CWE-78] en FortiSwitch podría permitir que un atacante local autenticado ejecute código no autorizado a través de la CLI de FortiSwitch.
14/01/2024	Fortinet	CVE-2024-48884 CVE-2024-48885	7.1	Una vulnerabilidad de limitación incorrecta de una ruta de acceso a un directorio restringido ('traversal de ruta') [CWE-22] en FortiManager, FortiOS, FortiProxy, FortiRecorder, FortiVoice y FortiWeb podría permitir que un atacante remoto autenticado con acceso a la interfaz y puerto de Security Fabric escriba archivos arbitrarios, y que un atacante remoto no autenticado con el mismo acceso a la red elimine una carpeta arbitraria.
14/01/2024	Fortinet	CVE-2024-35273	7.0	Una vulnerabilidad de escritura fuera de los límites [CWE-787] en el demonio sndproxy de FortiManager y FortiAnalyzer podría permitir que un atacante autenticado ejecute código o comandos arbitrarios a través de solicitudes HTTP especialmente manipuladas.
14/01/2024	Fortinet	CVE-2024-46670	7.5	Una vulnerabilidad de lectura fuera de los límites [CWE-125] en el servicio IPsec IKE del inquilino FortiOS y FortiSASE de FortiOS podría permitir que un atacante remoto no autenticado provoque un consumo de memoria que conduzca a una denegación de servicio mediante solicitudes manipuladas.
14/01/2024	Fortinet	CVE-2024-50566	7.2	Una vulnerabilidad de neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo ('Inyección de Comandos del Sistema Operativo') [CWE-78] en FortiManager podría permitir que un atacante remoto autenticado ejecute código no autorizado a través de solicitudes manipuladas de FGFM.
14/01/2024	Fortinet	CVE-2024-46668	7.1	Una vulnerabilidad de asignación de recursos sin límites ni regulación [CWE-770] en algunos puntos finales de la API de FortiOS podría permitir que un usuario remoto no autenticado consuma toda la memoria del sistema mediante múltiples cargas de archivos grandes.
14/01/2024	Fortinet	CVE-2024-35277	8.4	Una vulnerabilidad de falta de autenticación para una función crítica [CWE-306] en FortiManager y FortiPortal podría permitir que un atacante remoto no autenticado extraiga la configuración de todos los dispositivos gestionados.
14/01/2024	Fortinet	CVE-2024-23106	7.7	Una vulnerabilidad de restricción incorrecta de intentos excesivos de autenticación [CWE-307] en FortiClientEMS podría permitir que un atacante no autenticado intente realizar un ataque de fuerza bruta contra la consola de FortiClientEMS mediante solicitudes manipuladas de HTTP o HTTPS.
14/01/2024	Fortinet	CVE-2024-46662	8.3	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiManager csfd daemon may allow an authenticated attacker to execute unauthorized commands via specifically crafted packets
14/01/2024	Fortinet	CVE-2023-4863	7.1	El equipo de seguridad de productos de Fortinet ha evaluado el impacto de la vulnerabilidad que afecta a la biblioteca de Google Chrome
14/01/2024	Fortinet	CVE-2024-36512	7.0	Una vulnerabilidad de traversal de ruta relativa [CWE-23] en FortiManager y FortiAnalyzer podría permitir que un atacante privilegiado con perfil de superadministrador y acceso a la CLI escriba archivos en el sistema subyacente mediante solicitudes HTTP o HTTPS manipuladas.
14/01/2024	Fortinet	CVE-2024-47571	7.9	Una vulnerabilidad de operación en un recurso después de su expiración o liberación [CWE-672] en FortiManager podría permitir que una cuenta de administrador de FortiGate que haya sido eliminada a través de FortiManager aún pueda iniciar sesión en el FortiGate utilizando credenciales válidas.

EL RANSOMWARE FUNKSEC, IMPULSADO POR IA, ATACA A 85 VÍCTIMAS CON TÁCTICAS DE DOBLE EXTORSIÓN

FunkSec es una nueva y emergente familia de ransomware que, a diferencia de otros grupos similares, emplea inteligencia artificial (IA) para optimizar el desarrollo y la ejecución de sus ataques. Surgió a fines de 2024 y ya ha afectado a más de 85 víctimas, principalmente en países como Estados Unidos, India, Italia, Brasil e Israel. Su táctica principal es la doble extorsión, donde combinan el robo de datos y el cifrado de archivos para presionar a las víctimas a pagar rescates, los cuales suelen ser relativamente bajos, con montos que en algunos casos no superan los 10,000 dólares. Además, el grupo ha implementado un modelo de "ransomware como servicio", lanzando un sitio web dedicado a centralizar sus actividades. En este sitio, ofrecen herramientas personalizadas, como ransomware a medida y servicios de ataque DDoS. FunkSec también se ha involucrado en el tráfico de datos robados, vendiéndolos a compradores interesados por precios que oscilan entre los 1,000 y 5,000 dólares.

El ATAQUE

El ataque de FunkSec se basa en un ransomware desarrollado en Rust, diseñado para recorrer todos los directorios y cifrar los archivos seleccionados de las víctimas. Antes de cifrar los datos, el malware eleva privilegios, desactiva controles de seguridad, elimina copias de seguridad y termina procesos y servicios esenciales, lo que dificulta la recuperación del sistema. Además, FunkSec emplea tácticas de doble extorsión, combinando el cifrado de archivos con el robo de información, para presionar a las víctimas a pagar el rescate mediante la amenaza de divulgar datos confidenciales.

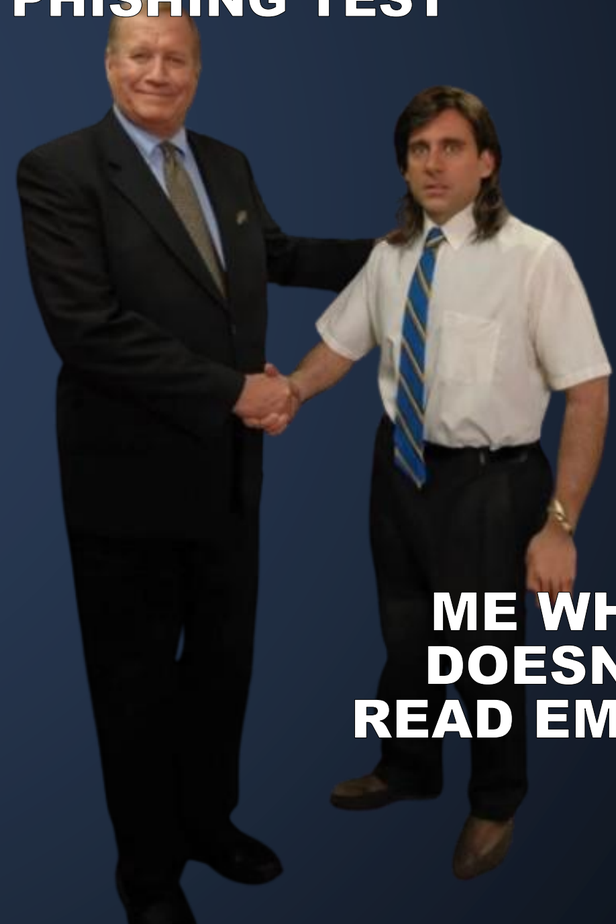
INFO

CONTEXT	INDICATOR	(MD5)
PE32+ executable (console) x86-64	e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22	039f85a7670428430274476cbe733db4
PE32+ executable (console) x86-64	dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac	2456fdd65bc48203815f22e444d78fb0
PE32+ executable (console) x86-64	b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb	54e383ca658ebd3caaf586f032f1c401
PE32+ executable (console) x86-64	66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd	61d7585b5702d195bc35e0be2f75915c
PE32+ executable (console) x86-64	5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd	834c7fd865eee5f7e17a3a1fb62e7051
PE32+ executable (console) x86-64	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c	c5c47f7a17ef4533d1c162042aa0313b
PE32+ executable (console) x86-64	20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d	c8dd54784fb1b6cbd16cec060487fb8f
PE32+ executable (console) x86-64	dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966	ca8ff8fb255a47d4be94af4ee3327c07
C source, ASCII text, with CRLF line terminators	7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603	f7a3a35cde86dc89bc76dbb59d5ce6de
PE32+ executable (console) x86-64	5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd	834c7fd865eee5f7e17a3a1fb62e7051
PE32+ executable (console) x86-64	dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac	2456fdd65bc48203815f22e444d78fb0
PE32+ executable (console) x86-64	dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966	ca8ff8fb255a47d4be94af4ee3327c07
PE32+ executable (console) x86-64	20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d	c8dd54784fb1b6cbd16cec060487fb8f

INFO

¡Lee tus correos... pero sin caer en trampas!

El phishing es una técnica utilizada por ciberdelincuentes para engañar a las personas mediante correos electrónicos que simulan ser comunicaciones legítimas, con el objetivo de robar información personal, contraseñas o datos financieros. Estos correos suelen incluir enlaces maliciosos, archivos adjuntos sospechosos o solicitudes urgentes de información sensible. Para protegerse, es importante verificar cuidadosamente el remitente, evitar hacer clic en enlaces o descargar archivos sin confirmar su autenticidad, y nunca proporcionar datos personales a través de correos no solicitados. Además, prestar atención a errores de redacción, direcciones de correo inusuales o mensajes que generen presión o urgencia puede ayudarte a identificar intentos de fraude. Mantente alerta y utiliza medidas de seguridad como autenticación en dos pasos y herramientas de protección para reducir los riesgos.



DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969