BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

WinRAR de día cero explotado para plantar malware en la extracción de archivos

TLP:CLEAR
19.08.2025

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → WinRAR de día cero explotado para plantar malware en la extracción de archivos

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.

Remote unauthenticated command injection

CVE-2025-25256

Critical (9.8)

Impacto: Inyección remota de comandos.

Resumen: Una neutralización incorrecta de elementos especiales utilizados en una vulnerabilidad de comando del sistema operativo ('OS Command Injection') [CWE-78] en FortiSIEM puede permitir que un atacante no autenticado ejecute código o comandos no autorizados a través de solicitudes CLI diseñadas.

Versiones Afectadas

- FortiSIEM 7.3 De 7.3.0 a 7.3.1
- FortiSIEM 7.2 De 7.2.0 a 7.2.5
- FortiSIEM 7.1 De 7.1.0 a 7.1.7
- FortiSIEM 7.0 De 7.0.0 a 7.0.3
- FortiSIEM 6.7 De 6.7.0 a 6.7.9
- FortiSIEM 6.6 Todas las versiones

Solución:

- Actualizar a la versión 7.3.2 o superior.
- Actualizar a la versión 7.2.6 o superior.
- Actualizar a 7.1.8 o superior
- Actualizar a la versión 7.0.4 o superior.

Ver +INFO.

Fecha de Publicación: 12/AGO/2025 +INFO

Weak authentication - FGFM protocol

CVE-2024-26009

Critical (7.9)

Impacto: Ejecución de código no autorizado.

Resumen: Una omisión de autenticación utilizando una vulnerabilidad de ruta o canal alternativo [CWE-288] en FortiOS, FortiProxy y FortiPAM puede permitir que un atacante no autenticado tome el control de un dispositivo administrado a través de solicitudes FGFM elaboradas, si el dispositivo es administrado por un FortiManager y si el atacante conoce el número de serie de FortiManager.

Versiones Afectadas

- FortiOS 6.4 De 6.4.0 a 6.4.15
- FortiOS 6.2 De 6.2.0 a 6.2.16
- FortiOS 6.0 6.0 Todas las versiones
- FortiPAM 1.2 1.2 Todas las versiones

Solución:

- Actualizar a la versión 6.4.16 o superior.
- Actualizar a la versión 6.2.17 o superior.
- Migrar a una versión fija

Ver +INFO.

Fecha de Publicación: 12/AGO/2025 +INFO

Cisco Secure Firewall Management Center Software RADIUS Remote Code Execution Vulnerability

CVE-2025-20265

Critical (10)

Impacto: Ejecución remota de código.

Resumen: Una vulnerabilidad en la implementación del subsistema RADIUS del software Cisco Secure Firewall Management Center (FMC) podría permitir que un atacante remoto no autenticado inyecte comandos de shell arbitrarios ejecutados por el dispositivo.

Versiones Afectadas

Esta vulnerabilidad afecta solo a las versiones 7.0.7 y 7.7.0 del software Cisco Secure FMC si tienen habilitada la autenticación RADIUS.

Solución:

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

Ver +INFO.

Fecha de Publicación: 14/AGO/2025 INFO

Cisco Secure Firewall Threat Defense Software Snort 3 Denial of Service Vulnerability

CVE-2025-20217

High (8.6)

Impacto: Denegación de servicio (DoS).

Resumen: Una vulnerabilidad en la funcionalidad de inspección de paquetes del motor de detección Snort 3 del software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.

Versiones Afectadas

Esta vulnerabilidad afecta a los dispositivos Cisco si ejecutan una versión vulnerable del software Cisco Secure FTD y tienen habilitada una política de intrusión que tiene el motor Snort 3 en ejecución.

Solución:

Cisco ha lanzado actualizaciones de software gratuitas que abordan la vulnerabilidad descrita en este aviso.

Ver +INFO.

Fecha de Publicación: 14/AGO/2025 INFO

Actualización de seguridad para Dell Networking OS10

CVE-2024–38428, CVE-2023–4738, CVE-2025–4802, CVE-2024-3596, CVE-2020-7105

La corrección de Dell Networking OS10 está disponible para múltiples vulnerabilidades de seguridad que podrían ser explotadas por usuarios malintencionados para comprometer el sistema afectado.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

Dell Networking OS10, versiones anteriores a 10.5.6.10

Ver +INFO

Fecha de Publicación: 7/AGO/2025 INFO

Actualizaciones de seguridad de Android

CVE-2025-22441, CVE-2025-48533, CVE-2025-48530, CVE-2025-0932, CVE-2025-27038

Google ha lanzado actualizaciones de seguridad en agosto para corregir múltiples vulnerabilidades que afectan al sistema operativo Android. Un actor malicioso podría explotar algunas de estas vulnerabilidades para lograr la elevación de privilegios o la ejecución remota de código.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

AOSP, versiones 13, 14, 15, 16 con parches de seguridad anteriores a agosto de 2025.

Ver +INFO

Fecha de Publicación: 4/AGO/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
12/08/2025	CVE-2025-20222	CISCO	8.6	Una vulnerabilidad en la función de proxy RADIUS para la función VPN IPsec del software Cisco Secure Firewall Adaptive Security Appliance (ASA) y el software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS).
14/08/2025	CVE-2025-20244	CISCO	7.7	Una vulnerabilidad en el servicio VPN SSL de acceso remoto para el software Cisco Secure Firewall Adaptive Security Appliance (ASA) y el software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto autenticado como usuario de VPN haga que el dispositivo se vuelva a cargar inesperadamente, lo que resulta en una condición de denegación de servicio (DoS).
14/08/2025	CVE-2025-20133	CISCO	8.6	Múltiples vulnerabilidades en los servidores web de administración y VPN para el software Cisco Secure Firewall Adaptive Security Appliance (ASA) y el software Cisco Secure Firewall Threat Defense (FTD) podrían permitir que un atacante remoto no autenticado haga que el dispositivo deje de responder o se vuelva a cargar inesperadamente, lo que resulta en una condición de denegación de servicio (DoS).
14/08/2025	CVE-2025-20134	CISCO	8.6	Una vulnerabilidad en el procesamiento de certificados del software Cisco Secure Firewall Adaptive Security Appliance (ASA) y el software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto no autenticado haga que el dispositivo se vuelva a cargar inesperadamente, lo que resulta en una condición de denegación de servicio (DoS).
12/08/2025	CVE-2025-53744	FORTINET	6.8	Una vulnerabilidad de asignación de privilegios incorrecta [CWE-266] en FortiOS Security Fabric puede permitir que un atacante autenticado remoto con altos privilegios escale sus privilegios a superadministrador mediante el registro del dispositivo en un FortiManager malicioso.
12/08/2025	CVE-2023-45584	FORTINET	6.3	Una vulnerabilidad de doble liberación de memoria [CWE-415] en las interfaces administrativas de FortiOS, FortiProxy y FortiPAM podría permitir a un atacante con privilegios ejecutar código o comandos mediante solicitudes HTTP o HTTPS especialmente diseñadas.
12/08/2025	CVE-2024-52964	FORTINET	5.2	Una limitación incorrecta de una vulnerabilidad de nombre de ruta a un directorio restringido ('Path Traversal') [CWE-22] en FortiManager y FortiManager Cloud puede permitir que un atacante remoto autenticado sobrescriba archivos arbitrarios a través de solicitudes creadas por FGFM.

WinRAR de día cero explotado para plantar malware en la extracción de archivos

Una vulnerabilidad de WinRAR recientemente corregida rastreada como CVE-2025-8088 fue explotada como un día cero en ataques de phishing para instalar el malware RomCom. Como WinRAR no incluye una función de actualización automática, se recomienda que todos los usuarios descarguen e instalen manualmente la última versión de win-rar.com para que estén protegidos de esta vulnerabilidad. Estos archivos explotaron el CVE-2025-8088 para ofrecer puertas traseras de RomCom. RomCom es un grupo alineado con Rusia".RomCom (también rastreado como Storm-0978, Tropical Scorpius o UNC2596) es un grupo de piratas informáticos ruso vinculado a ataques de ransomware y extorsión de robo de datos, junto con campañas centradas en el robo de credenciales.

El grupo es conocido por su uso de vulnerabilidades de día cero en ataques y el uso de malware personalizado para su uso en ataques de robo de datos, persistencia y para actuar como puertas traseras.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral.

Ver +INFO.

El ATAQUE

La falla corresponde a una vulnerabilidad de cruce de directorios corregida en WinRAR 7.13, la cual permite que un archivo especialmente diseñado extraiga contenido en una ruta elegida por el atacante, en lugar de la seleccionada por el usuario. En versiones anteriores de WinRAR, así como en las versiones para Windows de RAR, UnRAR, el código fuente portátil de UnRAR y la biblioteca UnRAR.dll, era posible engañar al programa para que utilizara una ruta definida dentro del archivo malicioso. Aprovechando esta debilidad, un atacante puede crear archivos que extraigan ejecutables directamente en rutas de ejecución automática del sistema. La próxima vez que un usuario inicie sesión, el ejecutable se ejecutará sin intervención, lo que posibilita la ejecución remota de código y potencialmente compromete el sistema afectado

INFO

CONTEXT	INDICATOR	(MD5)
CVE	CVE-2023-36884	N/A
CVE	CVE-2025-8088	N/A
IPV4	185.173.235.134	N/A
IPV4	194.36.209.127	N/A
URL	https://campanole[.]com/TOfrPOseJKZ	N/A
URL	https://melamorri[.]com/iEZGPctehTZ	N/A
DOMAIN	campanole[.]com	N/A
DOMAIN	gohazeldale[.]com	N/A
FileHash-SHA1	ab79081d0e26ea278d3d45da247335a545d0512e	ffa24cb3547347a9b442d8015bf56f82
FileHash-SHA1	ae687bef963cb30a3788e34cc18046f54c41ffba	4c458b976b583cda61aa8fa2827ab2cc
FileHash-SHA1	1aea26a2e2a7711f89d06165e676e11769e2fd68	dfa98877f293a851421ef22fe1556336

INFO

ÚLTIMAS NOTICIAS

Ciberdelincuentes suplantan a Bancolombia usando datos personales y WhatsApp para robar información bancaria. Una estafa bancaria se extiende en Bogotá y algunas partes de Colombia, donde delincuentes suplantan a Bancolombia a través de llamadas y WhatsApp, utilizando datos personales filtrados para engañar a las víctimas. Esta técnica busca robar credenciales de acceso, poniendo en riesgo el dinero de los usuarios.

INFO

El phishing nativo entrega contenido malicioso de una manera que se siente completamente legítima para la víctima. En este caso, por ejemplo, se envió a través del sistema de intercambio de archivos de M365, el archivo no se escanea como archivos adjuntos, se siente nativo y es una forma menos común de suplantar a los usuarios.
Todo lo que se necesita es un usuario interno comprometido y, de repente, toda la organización está en riesgo.

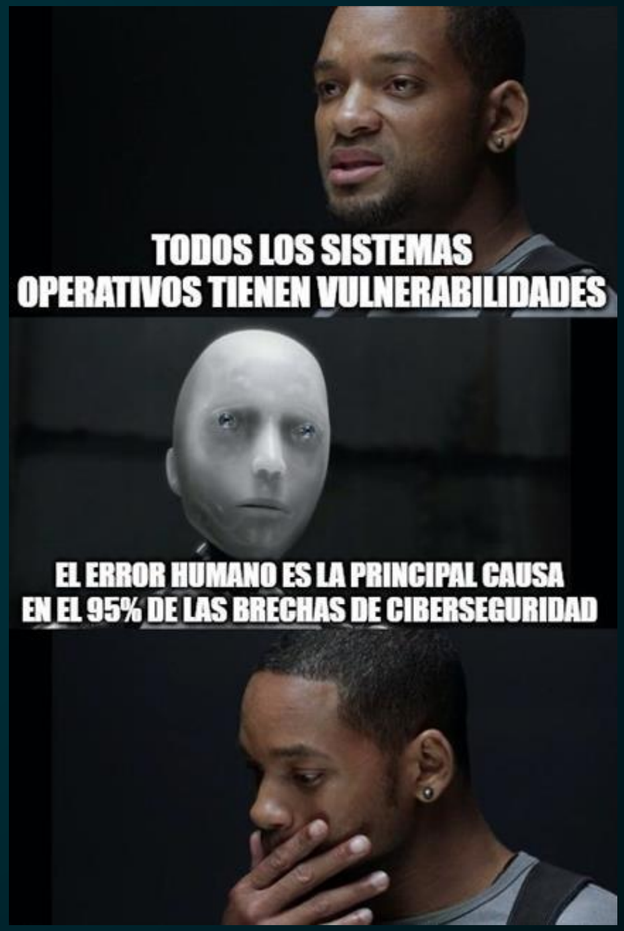
INFO

Las vulnerabilidades de firmware de ControlVault3 que afectan a más de 100 modelos de portátiles Dell pueden permitir a los atacantes eludir el inicio de sesión de Windows e instalar malware que persiste en las reinstalaciones del sistema. Dell ControlVault es una solución de seguridad basada en hardware que almacena contraseñas, datos biométricos y códigos de seguridad dentro del firmware en una placa secundaria.

INFO

🔐 Tu peor vulnerabilidad no está en tu sistema operativo... está en tus hábitos digitales.

La mayoría de las personas cree que las brechas de ciberseguridad ocurren por culpa de hackers altamente capacitados o virus sofisticados. Pero la realidad es más simple (y más preocupante) de los incidentes de seguridad ocurren por error humano.
Sí, los sistemas operativos tienen fallas. Pero lo que realmente abre la puerta a los ataques es que usamos la misma contraseña para todo, las guardamos en notas del celular, o las compartimos sin pensar por mensajes, redes sociales o correos.
🔎 ¿Te suena familiar?
“Solo se la pasé a un amigo de confianza.”
“La anoté en un archivo... pero nadie más usa mi compu.”
“Me llegó un enlace raro, pero decía que era urgente.”
“Olvidé mi contraseña, la estoy buscando en Google...”
⚠️ La confianza excesiva, la prisa y la desinformación son tus peores enemigos digitales.
🧠 Recuerda: la seguridad digital empieza por ti. Proteger tus datos no se trata solo de tener buenos sistemas, sino de tener buenos hábitos.



DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 285 8969