BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Generadores de videos con IA falsos distribuyen nuevo malware infostealer Noodlophile

TLP:CLEAR

16.05.2025

CLICK PARA EMPEZAR

En esta edición: → Generadores de videos con IA falsos distribuyen nuevo malware infostealer Noodlophile

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 IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability

CVE-2025-20188

Critical (10)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad en la funcionalidad de descarga de imágenes de punto de acceso (AP) Out-of-Band del software Cisco IOS XE para Wireless LAN Controllers (WLCs) podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios en un sistema afectado.

Versiones Afectadas

- Catalyst 9800-CL para la nube
- Catalyst 9800 para switches Catalyst de las series 9300, 9400 y 9500
- Catalyst serie 9800
- Controlador inalámbrico integrado en puntos de acceso Catalyst.

Solución: Los administradores pueden deshabilitar la función de descarga de imágenes de AP fuera de banda.

Ver +INFO.

Fecha de Publicación: 7/MAY/2025 INFO

Cisco IOS XE Software Web-Based Management Interface Command Injection Vulnerability

CVE-2025-20186

High (8.8)

Impacto: Inyección de comandos.

Resumen: Una vulnerabilidad en la interfaz de administración basada en web de la función Wireless LAN Controller del software Cisco IOS XE podría permitir a un atacante remoto autenticado, con una cuenta de usuario tipo *lobby ambassador*, ejecutar un ataque de inyección de comandos contra un dispositivo afectado.

Versiones Afectadas

Controladores inalámbricos

- Catalyst 9800-CL para la nube.
- Catalyst 9800 para switches
- Catalyst de las series 9300, 9400 y 9500
- Catalyst serie 9800.

Solución: Los administradores pueden deshabilitar la cuenta de tipo *lobby ambassador* para eliminar el vector de ataque de esta vulnerabilidad.

Ver +INFO.

Fecha de Publicación: 7/MAY/2025 INFO

Cisco IOS, IOS XE, and IOS XR Software TWAMP Denial of Service Vulnerability

CVE-2025-20154

High (8.6)

Impacto: Denegación de servicios.

Resumen: Una vulnerabilidad en la función del servidor del Protocolo de medición activa bidireccional (TWAMP) del software Cisco IOS y el software Cisco IOS XE podría permitir que un atacante remoto no autenticado haga que el dispositivo afectado se recargue, lo que resulta en una condición de denegación de servicio (DoS).

Versiones Afectadas

- El software IOS se ve afectado con o sin depuraciones habilitadas.
- IOS XE Software las versiones 16.6.1 a 17.2.3.
- El software IOS XR se ve afectado únicamente si el comando de depuración debug ipsla trace twamp connection está activo.

Solución: Cisco ha lanzado actualizaciones de software gratuitas que corrigen la vulnerabilidad descrita en este aviso.

Ver +INFO.

Fecha de Publicación: 7/MAY/2025 INFO

Cisco IOS XE Software for WLC Wireless IPv6 Clients Denial of Service Vulnerability

CVE-2025-20140

High (7.4)

Impacto: Denegación de servicios.

Resumen: Una vulnerabilidad en el Wireless Network Control daemon (wncd) del software Cisco IOS XE para controladores de LAN inalámbrica (WLC) podría permitir que un atacante inalámbrico adyacente no autenticado cause una condición de denegación de servicio (DoS).

Versiones Afectadas

- Controladores inalámbricos integrados Catalyst 9800 para switches Catalyst de las series 9300, 9400 y 9500
- Catalyst serie 9800
- Catalyst 9800-CL para la nube
- Controladores inalámbricos integrados en puntos de acceso Catalyst.

Solución: Cisco ha lanzado actualizaciones de software gratuitas que corrigen la vulnerabilidad descrita en este aviso.

Ver +INFO.

Fecha de Publicación: 7/MAY/2025 INFO

Stack-based buffer overflow vulnerability in API

CVE-2025-32756

Critical (9.6)

Impacto: Ejecución remota de código.

Resumen: Una vulnerabilidad de desbordamiento basada en pila en FortiVoice, FortiMail, FortiNDR, FortiRecorder y FortiCamera puede permitir que un atacante remoto no autenticado ejecute código arbitrario o comandos a través de solicitudes HTTP elaboradas.

Versiones Afectadas

- FortiMail 7.6 de 7.6.0 a 7.6.2
- FortiMail 7.4 de 7.4.0 a 7.4.4
- FortiMail 7.2 de 7.2.0 a 7.2.7
- FortiMail 7.0 de 7.0.0 a 7.0.8
- FortiNDR 7.6 7.6.0
- FortiNDR 7.4 De 7.4.0 a 7.4.7
- FortiNDR 7.2 De 7.2.0 a 7.2.4
- FortiNDR 7.1 7.1 Todas las versiones.

Solución:

- Actualización a 7.6.3 o superior
- Actualización a 7.4.5 o superior
- Actualización a la versión 7.2.8 o superior
- Actualización a 7.0.9 o superior
- Actualización a 7.6.1 o superior
- Actualización a 7.4.8 o superior
- Actualización a 7.2.5 o superior
- Migración a una versión fija.

Ver +INFO.

Fecha de Publicación: 13/MAY/2025 INFO

TACACS+ authentication bypass

CVE-2025-22252

Critical (9.0)

Impacto: Denegación de servicios.

Resumen: Una autenticación faltante para la vulnerabilidad de función crítica [CWE-306] en FortiOS, FortiProxy y FortiSwitchManager TACACS+ configurado para usar un servidor TACACS+ remoto para la autenticación, que a su vez se ha configurado para usar la autenticación ASCII, puede permitir que un atacante con conocimiento de una cuenta de administrador existente acceda al dispositivo como un administrador válido a través de una omisión de autenticación.

Versiones Afectadas

- FortiSwitchManager 7.2 .5
- FortiOS 7.6.0
- FortiOS 7.4 de 7.4.4 a 7.4.6
- FortiProxy 7.6 de 7.6.0 a 7.6.1

Solución:

- Actualización a 7.2.6 o superior
- Actualización a 7.6.1 o superior
- Actualización a 7.4.7 o superior
- Actualización a 7.6.2 o superior

Ver +INFO.

Fecha de Publicación: 8/MAY/2025 INFO

Actualización de Seguridad para Oracle

CVE-2025–22477, CVE-2025-22478, CVE-2025-22479, CVE-2025-23379, CVE-2025-22476

Se identificaron múltiples vulnerabilidades en el Dell Storage Center – Dell Storage Manager. Un actor malicioso remoto podría explotar estas vulnerabilidades para provocar inyección de scripts, elevación de privilegios o manipulación de información.

Recomendación:
Actualizar a la versión 2020 R1.21 o posterior.

Versiones Afectadas

Versiones anteriores a 2020 R1.21

Fecha de Publicación: 6/MAY/2025

Actualizaciones de seguridad mensuales para Android

CVE-2025-27363, CVE-2023-21342, CVE-2024-34739, CVE-2025-0077, CVE-2025-0087, CVE-2025-22425

Google ha lanzado sus actualizaciones de seguridad mensuales para Android con correcciones para 46 vulnerabilidades, incluida una que podría haber sido explotada. Esta podría llevar a la ejecución de código local sin requerir privilegios de ejecución adicionales. También resuelve otras ocho vulnerabilidades en el sistema Android y 15 en el módulo Framework que podrían usarse para facilitar la escalada de privilegios, la divulgación de información o la denegación de servicio.

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

Versiones Afectadas

AOSP versiones 13,14 y 15.

Fecha de Publicación: 5/MAY/2025

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
7/05/2025	CVE-2025-20213	CISCO	5.5	Una vulnerabilidad en la CLI de Cisco Catalyst SD-WAN Manager, anteriormente Cisco SD-WAN vManage, podría permitir que un atacante local autenticado sobrescriba archivos arbitrarios en el sistema de archivos local de un dispositivo afectado. Para aprovechar esta vulnerabilidad, el atacante debe tener credenciales válidas de solo lectura con acceso CLI en el sistema afectado.
7/05/2025	CVE-2025-20193	CISCO	6.5	Múltiples vulnerabilidades en la interfaz de administración basada en web del software Cisco IOS XE podrían permitir que un atacante remoto lea archivos del sistema operativo subyacente, lea partes limitadas del archivo de configuración, borre el syslog o realice un ataque de falsificación de solicitudes entre sitios (CSRF) en un dispositivo afectado, según su nivel de privilegio.
7/05/2025	CVE-2025-20187	CISCO	6.5	Una vulnerabilidad en los terminales de datos de la aplicación de Cisco Catalyst SD-WAN Manager, anteriormente Cisco SD-WAN vManage, podría permitir que un atacante remoto autenticado escriba archivos arbitrarios en un sistema afectado.
7/05/2025	CVE-2025-20147	CISCO	5.4	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Catalyst SD-WAN Manager, anteriormente Cisco SD-WAN vManage, podría permitir que un atacante remoto autenticado realice un ataque de secuencias de comandos entre sitios (XSS) almacenado en un sistema afectado.
7/05/2025	CVE-2025-20216	CISCO	4.7	Una vulnerabilidad en la interfaz web de Cisco Catalyst SD-WAN Manager, anteriormente Cisco SD-WAN vManage, podría permitir que un atacante remoto no autenticado inyecte HTML en el navegador de un usuario autenticado.
7/05/2025	CVE-2025-20221	CISCO	5.3	Una vulnerabilidad en las funciones de filtrado de paquetes del software Cisco IOS XE SD-WAN podría permitir que un atacante remoto no autenticado omita los filtros de tráfico de capa 3 y capa 4.
7/05/2025	CVE-2025-20151	CISCO	4.3	Una vulnerabilidad en la implementación de la función Simple Network Management Protocol Versión 3 (SNMPv3) del software Cisco IOS y el software Cisco IOS XE podría permitir que un atacante remoto autenticado sondee un dispositivo afectado mediante SNMP, incluso si el dispositivo está configurado para denegar el tráfico SNMP de una fuente no autorizada o si el nombre de usuario SNMPv3 se elimina de la configuración.
13/05/2025	CVE-2025-20214	FORTINET	4.8	Una vulnerabilidad de desbordamiento de enteros o envolvente [CWE-190] en FortiOS Security Fabric puede permitir que un atacante remoto no autenticado bloquee el demonio csfd a través de una solicitud especialmente diseñada.

Generadores de videos con IA falsos distribuyen nuevo malware infostealer Noodlophile

Las herramientas de generación de falsos videos, impulsadas por IA se están utilizando para distribuir una nueva familia de malware que roba información llamada 'Noodlophile', bajo la apariencia de contenido multimedia generado.

Los sitios web utilizan nombres atractivos como "Dream Machine" y se anuncian en grupos de alta visibilidad en Facebook, haciéndose pasar por herramientas avanzadas de IA que generan videos basados en los archivos de usuario cargados.

Aunque el uso de herramientas de IA para distribuir malware no es un concepto nuevo y ha sido adoptado por ciberdelincuentes experimentados, el descubrimiento de la última campaña de Morphisec introduce un nuevo Stealer de información en el panorama de amenazas.

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

El ATAQUE

Una vez que la víctima visita el sitio web malicioso y carga sus archivos, recibe un archivo ZIP que se supone que contiene un video generado por IA. En su lugar, el ZIP contiene un ejecutable con un nombre engañoso (Video Dream MachineAI.mp4.exe) y una carpeta oculta con varios archivos necesarios para las etapas posteriores. Si un usuario de Windows tiene las extensiones de archivo deshabilitadas (nunca haga eso), a simple vista, parecería un archivo de video MP4. Al hacer doble clic en el MP4 falso, se ejecutará una serie de ejecutables que eventualmente lanzarán un script por lotes (Document.docx/install.bat). A continuación, el script ejecuta 'srchost.exe', que ejecuta un script de Python ofuscado (randomuser2025.txt) obtenido de una dirección de servidor remoto codificada, y finalmente ejecuta el Noodlophile Stealer en la memoria.

INFO

CONTEXT	INDICATOR	(MD5)
PEXE - PE32+ executable (console)	18c14dcfb9a54c5359026a5fcbdb3e4ba6ced2628a9cd9ae589baedbb29beaa6	f9baac5f7aef86ee1e331bd9cf004969
ASCII text, with very long lines, with CRLF line terminators	11c873cee11fd1d183351c9cdf233cf9b29e28f5e71267c2cb1f373a564c6a73	7e1ed90c0492da59c8fe87dac53c4182
PEXE - PE32+ executable (console) x86-64	18c14dcfb9a54c5359026a5fcbdb3e4ba6ced2628a9cd9ae589baedbb29beaa6	f9baac5f7aef86ee1e331bd9cf004969
IPv4	103.232.54.13	N/A
IPv4	160.25.232.62	N/A
IPv4	85.209.87.207	N/A
URL	http://103.232.54.13:25902	N/A
URL	http://160.25.232.62/bee/bee02_ads.txt	N/A
URL	http://lumalabs-dream.com/VideoLumaAI.zip	N/A
URL	https://85.209.87.207/sysdi/LDXC10.txt	N/A
URL	https://85.209.87.207/sysdi/randomuser2025.txt	N/A
URL	https://luma-aidreammachine.com/Creation_Luma.zip	N/A

INFO

🔐 Seguridad sin excepciones: Proteger la empresa empieza desde arriba 🔒

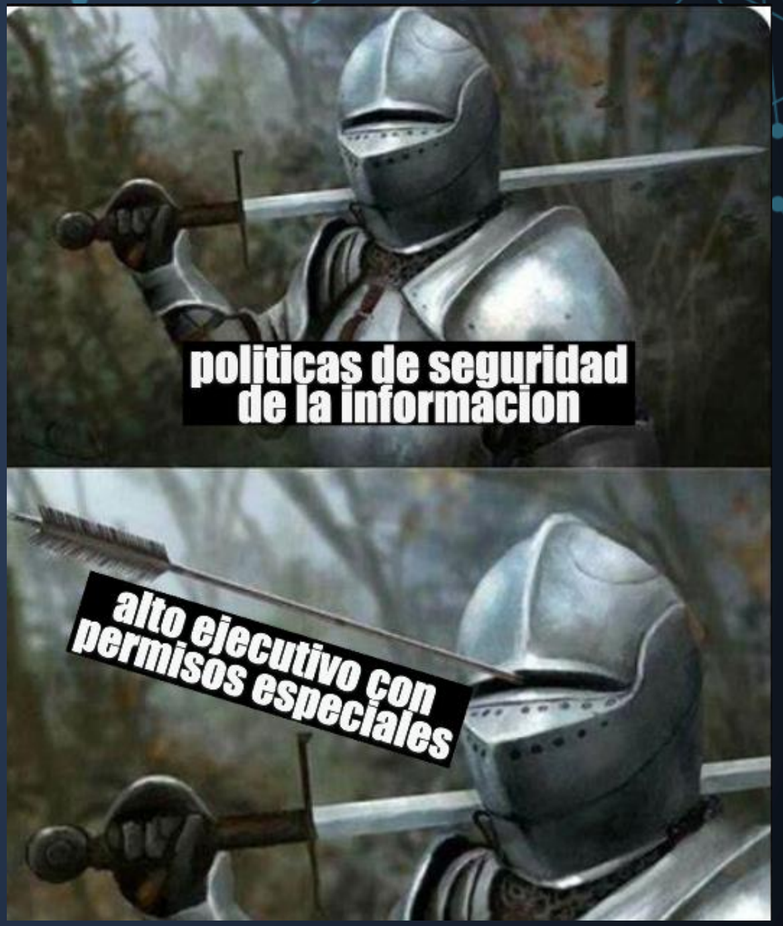
En muchas organizaciones, existe la tentación de otorgar permisos especiales a altos ejecutivos con el argumento de que necesitan "fluidez", "acceso total" o "agilidad para la toma de decisiones". Aunque suene lógico, esta práctica representa un riesgo crítico para la seguridad de toda la empresa.

🎯 Los delincuentes digitales buscan cuentas con más poder y acceso. ¿Quién mejor que un CEO o un director para abrirles la puerta al sistema?

🛡️ Más permisos = mayor riesgo, cada permiso adicional es una posible entrada para amenazas. No importa quién lo tenga.

🔄 Cuando los líderes no siguen las reglas, el resto del equipo puede relajarse también. La seguridad es un trabajo colectivo.

Para garantizar la integridad del entorno corporativo, es fundamental que los controles de seguridad se apliquen de manera uniforme, sin excepciones ni privilegios basados en jerarquía.



DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969