BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Piratas informáticos usan facturas falsas para propagar Xworm RAT a través de archivos de office

TLP:CLEAR
01.10.2025

CLICK PARA EMPEZAR

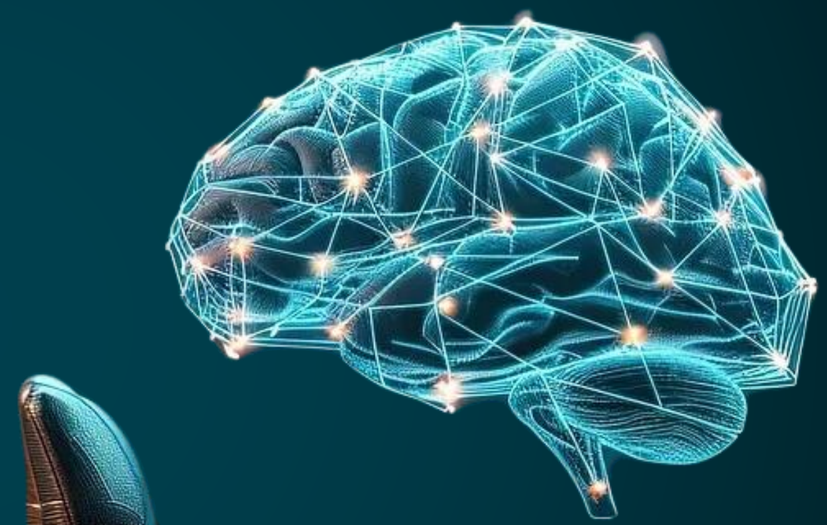
CYBERSOCDTS

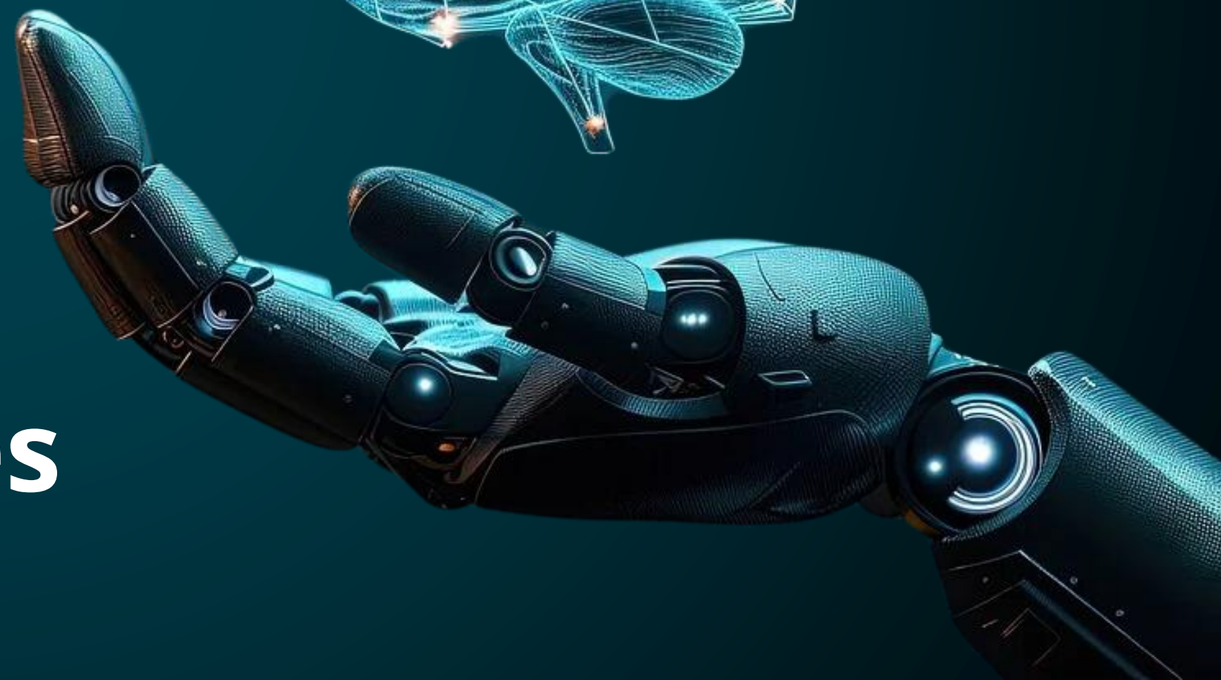
En esta edición: → Piratas informáticos usan facturas falsas para propagar Xworm RAT a través de archivos de office

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 Code Execution Vulnerability in the VPN Web Server of Cisco Secure Firewall ASA and FTD

CVE-2025-20333

critical (9.9)

Impacto: Ejecución remota de código.

Resumen: Una vulnerabilidad en el servidor web VPN del software Cisco Secure Firewall Adaptive Security Appliance (ASA) y del software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto autenticado ejecute código arbitrario en un dispositivo afectado.

Versiones Afectadas

Esta vulnerabilidad afecta a los dispositivos Cisco que ejecutan una versión vulnerable del software Cisco Secure Firewall ASA o del software Cisco Secure FTD, y que además tienen una o más de las configuraciones vulnerables. Para más detalles, consulte la sección *+INFO*.

Solución:

Cisco ha publicado actualizaciones de software gratuitas que solucionan la vulnerabilidad descrita en este boletín.

Ver +INFO.

Fecha de Publicación: 25/SEP/2025 INFO

Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability

CVE-2025-20160

High (8.1)

Impacto: Acceso no autorizado.

Resumen: Una vulnerabilidad en la implementación del protocolo TACACS+ en Cisco IOS Software y Cisco IOS XE Software podría permitir que un atacante remoto no autenticado vea datos sensibles o evada la autenticación.

Versiones Afectadas

Esta vulnerabilidad afecta a los dispositivos Cisco que estén ejecutando una versión vulnerable de Cisco IOS y IOS XE Software, y que estén configurados para usar TACACS+ pero no tengan configurado el secreto compartido de TACACS+.

Solución:

Cisco ha lanzado actualizaciones de software que solucionan esta vulnerabilidad.

Ver +INFO.

Fecha de Publicación: 24/SEP/2025 INFO

Vulnerabilidades en Google Chrome

CVE-2025-10500, CVE-2025-10501, CVE-2025-10502

critical (9.8)

Impacto: Ejecución remota de código.

Resumen: Se han descubierto vulnerabilidades de severidad alta y crítica en Google Chrome. Un actor malicioso podría explotar algunas de estas vulnerabilidades para lograr la ejecución remota de código, la evasión de mecanismos de seguridad o la redirección de URL.

Versiones Afectadas

Windows Versiones anteriores a 140.0.7339.185/.186.
MAC Versiones anteriores a 140.0.7339.185/.186.
Linux, versiones anteriores a 140.0.7339.185.

Solución:

Actualizar a la última versión disponible a través del sitio web oficial del fabricante. Para más detalles, consulte la sección INFO

Ver +INFO.

Fecha de Publicación: 17/SEP/2025

Vulnerabilidades en productos Mozilla

CVE-2025-10533, CVE-2025-10537, CVE-2025-10536

High (8.8)

Impacto: Denegación de servicio.

Resumen: Se han descubierto múltiples vulnerabilidades de severidad alta en productos Mozilla. Un actor malicioso podría lograr la evasión de restricciones de seguridad, la divulgación de información o la ejecución remota de código.

Versiones Afectadas

Versiones anteriores a 140.3 de Firefox ESR y Thunderbird ESR, y versiones anteriores a 143 de Firefox y Thunderbird.

Solución:

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

Ver +INFO.

Fecha de Publicación: 16/SEP/2025

Actualización de seguridad para Dell PowerProtect

CVE-2024–45491, CVE-2024–45492,CVE-2025-0838

Dell ha lanzado una actualización de seguridad para PowerProtect Cyber Recovery. Esta aborda múltiples vulnerabilidades en componentes de terceros.

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

Versiones Afectadas

Versiones anteriores a 19.20.0.1 del software Cyber Recovery, y versiones anteriores a 15.4.0-9 y 1.5.0-63 de las actualizaciones del sistema operativo SLES 15 SP4 y SLES 12 SP5, respectivamente.

Ver +INFO

Fecha de Publicación: 15/SEP/2025 INFO

Actualizaciones de seguridad de Microsoft

CVE-2025-59251, CVE-2025-29834, CVE-2025-26633, CVE-2025-21335, CVE-2025-53791

Microsoft ha lanzado las actualizaciones de seguridad correspondientes al mes de septiembre, incluyendo 91 vulnerabilidades. Estas podrían permitir la denegación de servicio, la elevación de privilegios, la divulgación de información, entre otros.

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

Versiones Afectadas

Azure, Desktop Windows Manager, GitHub Copilot, Visual Studio, Graphics Kernel, Kernel Streaming WOW Thunk Service Driver, Kernel Transaction Manager, Microsoft Office, Microsoft Edge, Microsoft Exchange Server, Windows y otras aplicaciones de Microsoft.

Ver +INFO

Fecha de Publicación: 30/SEP/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
25/09/2025	CVE-2025-20362	Cisco	6.5	Una vulnerabilidad en el servidor web VPN del software Cisco Secure Firewall Adaptive Security Appliance (ASA) y del software Cisco Secure Firewall Threat Defense (FTD) podría permitir que un atacante remoto no autenticado acceda a puntos finales de URL restringidos relacionados con el acceso remoto VPN que, de lo contrario, deberían ser inaccesibles sin autenticación.
24/09/2025	CVE-2025-20365	Cisco	4.3	Una vulnerabilidad en el procesamiento de paquetes de anuncio de enrutador (RA) IPv6 del software de punto de acceso de Cisco podría permitir que un atacante adyacente no autenticado modifique la puerta de enlace IPv6 en un dispositivo afectado.
25/09/2025	CVE-2025-20240	Cisco	6.1	Una vulnerabilidad en la función de autenticación web del software Cisco IOS XE podría permitir que un atacante remoto no autenticado realice un ataque de secuencias de comandos entre sitios reflejado (XSS) en un dispositivo afectado.
25/09/2025	CVE-2025-20313	Cisco	6.7	Varias vulnerabilidades en el software Cisco IOS XE podrían permitir que un atacante local autenticado con privilegios de nivel 15 o un atacante no autenticado con acceso físico a un dispositivo afectado ejecute código persistente en el momento del arranque y rompa la cadena de confianza.
24/09/2025	CVE-2025-20160	Cisco	8.1	Una vulnerabilidad en la implementación del protocolo TACACS+ en el software Cisco IOS y Cisco IOS XE podría permitir que un atacante remoto no autenticado vea datos confidenciales o eluda la autenticación.
24/0972025	CVE-2025-20327	Cisco	7.7	Una vulnerabilidad en la interfaz de usuario web del software Cisco IOS podría permitir que un atacante remoto autenticado con bajos privilegios provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.
24/0972025	CVE-2025-20338	Cisco	6.0	Una vulnerabilidad en la CLI del software Cisco IOS XE podría permitir que un atacante local autenticado con privilegios administrativos ejecute comandos arbitrarios como root en el sistema operativo subyacente de un dispositivo afectado.
15/09/2025	CVE-2025-20339	Cisco	5.8	Una vulnerabilidad en el procesamiento de la lista de control de acceso (ACL) de paquetes IPv4 del software Cisco SD-WAN vEdge podría permitir que un atacante remoto no autenticado eluda una ACL configurada.
26/09/2025	CVE-2025-36144	IBM	3.3	IBM Lakehouse almacena información potencialmente confidencial en archivos de registro que un usuario local podría leer. Esto podría afectar a watsonx.data.
26/09/2025	CVE-2024-43192	IBM	6.5	Ciertos formularios HTML en la interfaz gráfica web no utilizaban tokens anti-CSRF, lo que permitía a los atacantes engañar a los usuarios autenticados para que realizaran acciones no deseadas. El problema se ha solucionado añadiendo protección CSRF a los formularios afectados.
26/09/2025	CVE-2025-36239	IBM	6.1	Esta vulnerabilidad permite a un atacante no autenticado incrustar código JavaScript arbitrario en la interfaz web, alterando así la funcionalidad prevista, lo que podría provocar la divulgación de credenciales en una sesión de confianza.

Piratas informáticos usan facturas falsas para propagar Xworm RAT a través de archivos de office

Una nueva campaña de phishing usa correos que simulan facturas pendientes de pago con un archivo adjunto .xlam. Al abrirlo se ejecuta un componente oculto que inicia la cadena de infección y, finalmente, se instala el RAT XWorm (Remote Access Trojan), capaz de obtener acceso remoto y exfiltrar información sensible del equipo.

La técnica aprovecha mecanismos ofuscados dentro del documento Office para evitar la detección inicial y aparentar un archivo corrupto o en blanco. La afectación principal es la pérdida de confidencialidad y control del endpoint comprometido; además, la campaña utiliza técnicas avanzadas (carga en memoria e inyección en procesos) que dificultan la detección por soluciones que solo analizan archivos en disco.

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

El ATAQUE

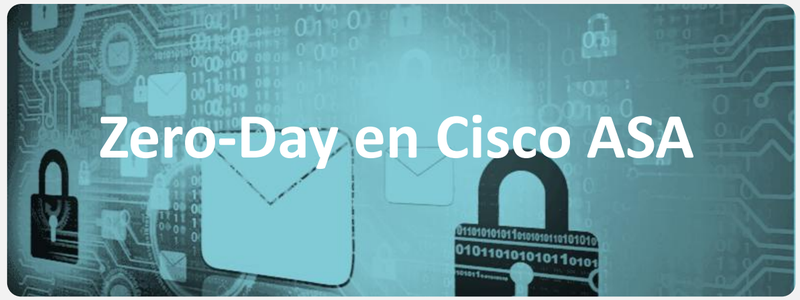
Dentro del archivo adjunto de Office hay un componente oculto llamado oleObject1.bin, que contiene un código cifrado, llamado shellcode. Este shellcode es un pequeño programa que descarga inmediatamente la siguiente parte del ataque. El shellcode accede a una dirección web específica, hxxp://alpinreisan1com/UXOexe, para descargar el programa malicioso principal, un archivo ejecutable llamado UXO.exe. Este programa inicia la segunda etapa: carga otro archivo DLL dañino en la memoria del ordenador (DriverFixPro.dll). Esta carga se realiza mediante inyección reflexiva de DLL (una forma disimulada de cargar un programa dañino directamente en la memoria del ordenador sin guardarlo previamente como un archivo normal). Esta DLL realiza una inyección de proceso, que consiste en forzar la ejecución del código malicioso dentro de un programa normal e inofensivo del ordenador. Este código inyectado final pertenece a la familia XWorm RAT.

INFO

CONTEXT	INDICATOR	(MD5)
domain	berlin101[.]com	N/A
IPv4	158[.]94[.]209[.]180	N/A
URL	http://alpinreisan1[.]com/UXO[.]exe	N/A
domain	alpinreisan1[.]com	N/A
domain	filesberlin101[.]com	N/A
PEXE - PE32 executable	a07218767cb37a2eb228ddf96d25724848f368c446abe6ad0813387dfc603f98	af22bb92639cb98b8f09382c32c478ac
PEXE - PE32 executable	a4b889611fad0ce73151c132017ef1e14c52d3d99b105937db3c433337b89063	6b4956c794ec81d31e89714da7600185
PEXE - PE32 executable	eb4710d9a5944b5f86bf3bd08ec933716f871f30e1adc0c9da44772d31fb6015	079207c335f700daf648bd36abe0b365

INFO

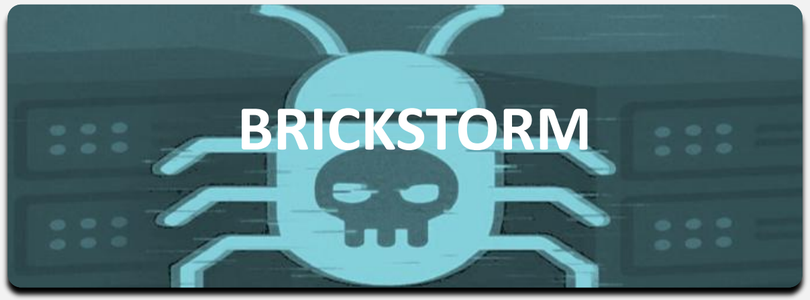
ÚLTIMAS NOTICIAS



Zero-Day en Cisco ASA

El NCSC del Reino Unido ha alertado sobre la explotación activa de vulnerabilidades recientemente descubiertas en los firewalls Cisco Secure ASA, utilizadas en ataques de Zero-Day para distribuir familias de malware no documentadas previamente, como RayInitiator y LINE VIPER. Los atacantes aprovechan estas fallas para eludir la autenticación y ejecutar código malicioso en dispositivos comprometidos. Un análisis forense del firmware de dispositivos infectados con servicios web VPN habilitados permitió identificar un error de corrupción de memoria en el software del firewall.

INFO



BRICKSTORM

Un grupo de piratas informáticos con vínculos con China ha sido identificado ejecutando una operación de espionaje prolongada contra empresas estadounidenses. La amenaza, conocida como BRICKSTORM, apunta a sistemas operativos como Linux y BSD para robar propiedad intelectual e información confidencial relacionada con la seguridad nacional y el comercio internacional. Los atacantes han mantenido el acceso a sistemas comprometidos por un promedio de 393 días, afectando a sectores como servicios legales, tecnología, SaaS y BPO.

INFO

Troyano oculto en TradingView Premium

Una campaña publicitaria maliciosa que ha estado engañando a los creadores de contenido y a los usuarios desprevenidos para que descarguen software dañino al ofrecer "acceso gratuito" a TradingView Premium ha expandido drásticamente sus operaciones, advierten los investigadores de seguridad. Esta campaña fue reportada anteriormente por Hackread.com por explotar los anuncios de Facebook utilizando sitios criptográficos falsos e imágenes de celebridades para propagar malware, pero ahora ha evolucionado sus tácticas.

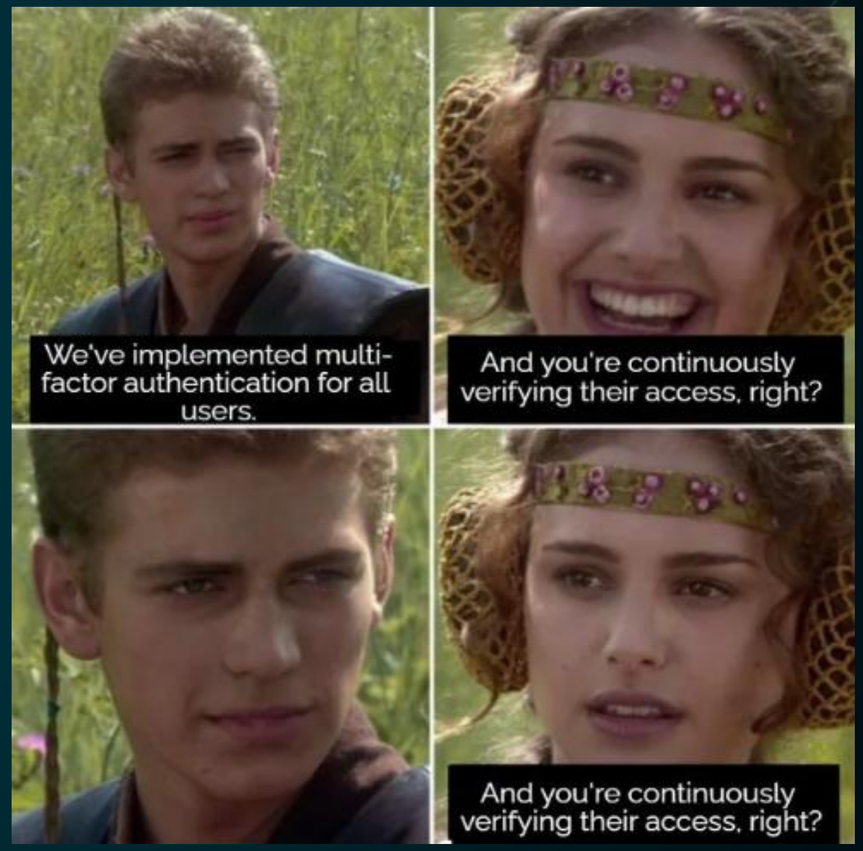
INFO

Controles vigentes, seguridad real el valor de la verificación constante

No basta con implementar controles de seguridad y darlos por sentados. La verdadera fortaleza está en la verificación continua: comprobar de manera periódica que esos controles siguen funcionando como se espera, que no han quedado obsoletos y que realmente están mitigando los riesgos actuales.

- ✅ Monitoreo constante: utilizar herramientas de auditoría y supervisión para validar el desempeño de los controles.
- 🔄 Pruebas periódicas: realizar simulaciones de incidentes, escaneos de vulnerabilidades y pruebas de penetración.
- 📊 Revisión de métricas: medir la efectividad de cada control frente a las amenazas que evolucionan día a día.
- 🗓️ Actualización oportuna: ajustar, corregir o reemplazar controles que ya no sean eficaces.
- 👥 Cultura de mejora continua: involucrar a los equipos para mantener la seguridad como un proceso vivo y no como una tarea puntual.

👉 Con estas prácticas, la MFA pasa de ser una simple barrera inicial a un mecanismo de defensa continuo, que protege de ataques como el account takeover, el phishing avanzado o la exfiltración de datos, fortaleciendo la resiliencia de las organizaciones en un entorno digital cada vez más hostil.



DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 315 9346 Ext. 4