



PolarEdge ataca enrutadores Cisco, ASUS, QNAP y Synology en una campaña de botnets en expansión





TLP:CLEAR
31.10.2025

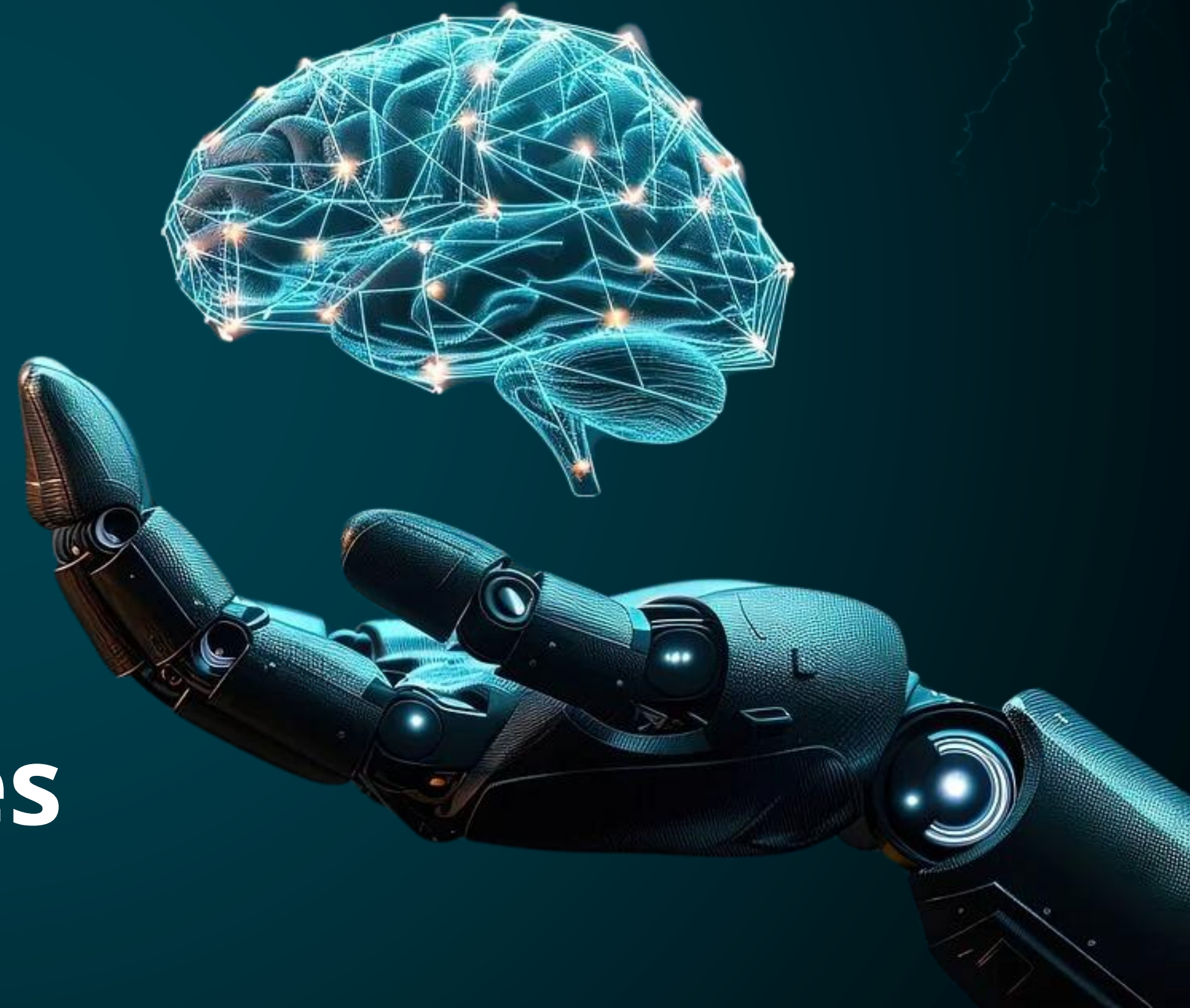
CLICK PARA
EMPEZAR



CONTENIDO



-  **Nuestra Esencia**
-  **Vulnerabilidades**
-  **Noticias**
-  **Recomendaciones**



NUESTRA ESENCIA



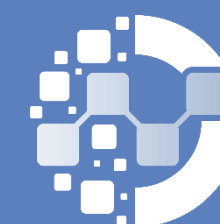
BOLETÍN CIBERSEGURIDAD

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.



Microsoft releases an emergency patch for the Windows Server vulnerability.

CVE-2025-59287



**Critical
(9.8)**

Impacto: Escalada de privilegios.

Resumen: Esta falla permite la ejecución arbitraria de código mediante la deserialización insegura de datos no confiables en un mecanismo heredado, potencialmente comprometiendo la confidencialidad, integridad y disponibilidad del sistema afectado.

Versiones Afectadas

La versión compatible afectada es:

- Windows Server Update Services.

[Ver +INFO.](#)

Solución:

Microsoft publicó un parche de emergencia y se recomienda implementarlo inmediatamente

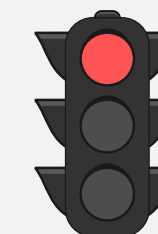
[Ver + INFO.](#)

Fecha de Publicación: 24/OCT/2025 [+INFO](#)



Google Chromium Mojo Sandbox Escape Vulnerability

CVE-2025-2783



**High
(8.3)**

Impacto: Escalada de privilegios.

Resumen: Un identificador incorrecto proporcionado en circunstancias no especificadas en Mojo en Google Chrome para Windows, antes de la versión 134.0.6998.177, permitía a un atacante remoto realizar una evasión del sandbox mediante un archivo malicioso.

Versiones Afectadas

La versión compatible afectada es:

- Google Chrome 134.0.6998.177

[Ver +INFO.](#)

Solución:

Actualizar Google Chrome a la última versión.

[Ver +INFO.](#)

Fecha de Publicación: 27/OCT/2025 [+INFO](#)



Vulnerability in the Oracle VM VirtualBox

CVE-2025-62587



High
(8.2)

Impacto: Escalada de privilegios.

Resumen: Se identificó una falla en el componente Core de Oracle VM VirtualBox que permite a un atacante con privilegios locales elevados comprometer el entorno y potencialmente afectar otros sistemas asociados. Su explotación exitosa puede derivar en la toma de control total de la aplicación.

Versiones Afectadas

La versión compatible afectada es:

- 7.1.12, 7.2.2

[Ver +INFO.](#)

Solución:

Aplicar el parche disponible para la plataforma.

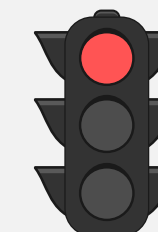
[Ver +INFO.](#)

Fecha de Publicación: 23/OCT/2025 [+INFO](#)



Tenable Identity Exposure Multiple Vulnerabilities

CVE-2025-55315, CVE-2025-55247
CVE-2025-55248



Critical
(9.9)

Impacto: Escalada de privilegios.

Resumen: Se identificaron vulnerabilidades en componentes de terceros (.NET) utilizados por Tenable Identity Exposure para su funcionamiento.

Versiones Afectadas

Las versiones compatibles afectadas son:

- Tenable Identity Exposure 3.93.3 y versiones anteriores.

[Ver +INFO.](#)

Solución:

Actualizar a la versión 3.93.4 de Tenable Identity Exposure para abordar estos problemas.

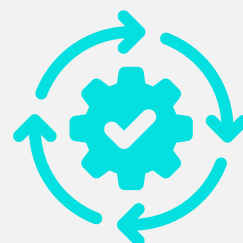
[Ver +INFO.](#)

Fecha de Publicación: 17/OCT/2025 [+INFO](#)



Actualización de Oracle

**CVE-2025-53036 - CVE-2025-53037 - CVE-2025-6965 -
CVE-2020-11988 - CVE-2025-61751- CVE-2025-48976**



Oracle ha lanzado actualización de parches para múltiples vulnerabilidades de código de Oracle y de componentes de terceros incluidos en los productos de Oracle.

Recomendación:

Aplicar los parches de seguridad para las aplicaciones de Oracle, ya que pueden explotarse de forma remota sin autenticación.

Versiones Afectadas

Las versiones compatibles afectadas son:

- Oracle Financial Services Analytical Applications Infrastructure:Versiones, 8.0.7.9, 8.0.8.7, 8.1.2.5
- Oracle Financial Services Compliance Studio: versions, 8.1.2.8
- Oracle Banking Branch: Versiones, 14.5.0.0.0-14.8.0.0.0

[Ver +INFO](#)

Fecha de Publicación: 24/OCT/2025 [+INFO](#)



Actualizaciones de Microsoft

CVE-2025-53770



Microsoft ha publicado actualizaciones que corrigen la vulnerabilidad CVE-2025-53770 en SharePoint.

Recomendación:

Priorizar la instalación inmediata del parche en los sistemas y limitar el acceso externo a SharePoint para mitigar riesgos adicionales.

Producto Afectado:

La versión compatible afectada es:

- SharePoint

[Ver +INFO](#)

Fecha de Publicación: 24/OCT/2025 [+INFO](#)

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
24/10/2025	CVE-2025-62868	Edge	8.1	Permite el acceso no autorizado a archivos y la ejecución de código no autorizado en un sistema, esto se debe a un control incorrecto de la cadena de nombres en un programa PHP.
30/10/2025	CVE-2025-58726	Windows	7.5	Se identificó una falla de control de acceso que podría permitir a un atacante con credenciales válidas aumentar sus privilegios de manera remota dentro de la red..
27/10/2025	CVE-2025-33073	Microsoft	8.8	Permite a un atacante autorizado elevar los privilegios sobre una red.
20/10/2025	CVE-2025-61884	Oracle	7.5	Permite que un atacante remoto, sin necesidad de autenticación, que tenga acceso de red al servicio HTTP, comprometa el módulo Oracle Configurator e inicie solicitudes que permitan acceder a datos sensibles o incluso todos los datos accesibles por ese módulo.
17/10/2025	CVE-2025-20350	Cisco	7.5	Se identificó una vulnerabilidad de desbordamiento de búfer en la interfaz web de los teléfonos Cisco (series 7800, 8800, 9800 y 8875) que podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) mediante el envío de paquetes HTTP manipulados.El riesgo aplica solo si el acceso web está habilitado y el dispositivo está registrado en CUCM.
17/10/2025	CVE-2025-20351	Cisco	6.1	Una validación insuficiente en la interfaz web de los teléfonos Cisco (series 7800, 8800, 9800 y 8875) podría permitir a un atacante remoto ejecutar código malicioso (XSS) o acceder a información sensible del usuario.El riesgo aplica solo si el acceso web está habilitado y el dispositivo está registrado en CUCM.
21/10/2025	CVE-2025-20307	Cisco	4.8	Podría permitir que un atacante remoto autenticado realice ataques de secuencias de comandos entre sitios (XSS) contra un usuario de la interfaz.
30/10/2025	CVE-2025-55680	Windows	7.8	Se identificó una condición de carrera (TOCTOU) que podría permitir a un atacante con acceso local aumentar sus privilegios en el sistema afectado.
16/10/2025	CVE-2025-58718	Microsoft	8.8	Se identificó una vulnerabilidad use-after-free que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en los sistemas afectados mediante una conexión de red.

PolarEdge ataca routers de Cisco, ASUS, QNAP y Synology

PolarEdge es una botnet detectada por primera vez en febrero de 2025 que compromete enrutadores Cisco, ASUS, QNAP y Synology para formar una red de dispositivos controlada remotamente. Emplea un implante ELF que usa TLS para enviar huellas del host al servidor C2 y ejecutar comandos recibidos mediante un protocolo binario personalizado. El ataque aprovecha la vulnerabilidad CVE-2023-20118 en enrutadores Cisco para descargar un script que instala la puerta trasera PolarEdge. Incluye modos de conexión y depuración, configuración ofuscada con XOR y técnicas anti-análisis y evasivas (por ejemplo, enmascaramiento de procesos). Aunque no persiste tras reinicios, implementa un proceso secundario que le permite auto-reiniciarse si el proceso principal es terminado.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver [+INFO](#).

EL ATAQUE

Los actores de amenazas explotan la falla de seguridad que afecta a los enrutadores para descargar un script de shell llamado "q" a través de FTP, que luego es responsable de recuperar y ejecutar la puerta trasera PolarEdge en el sistema comprometido. La función principal de la puerta trasera es enviar una huella digital del host a su servidor de comando y control y luego escuchar comandos a través de un servidor TLS incorporado implementado con mbedTLS.

PolarEdge está diseñado para admitir dos modos de operación: un modo de conexión, donde la puerta trasera actúa como un cliente TLS para descargar un archivo de un servidor remoto, y el modo de depuración, donde la puerta trasera entra en un modo interactivo para modificar su configuración (es decir, información del servidor) sobre la marcha.

CONTEXT	INDICATOR	(MD5)
IP	119[.]8[.]186[.]227	N/A
IP	195[.]123[.]212[.]54	N/A
IP	122[.]8[.]183[.]181	N/A
IP	43[.]129[.]205[.]244	N/A
IP	159[.]138[.]119[.]99	N/A
URL	asustordownload[.]com	N/A
SHA256	13cd040a7f488e937b1b234d71a0126b7bc74367bf6538b6961c476f5d620d13	d8f9da4dc52589871655f73a06bb5433
SHA256	464f29d5f496b4acffc455330f00adb34ab920c66ca1908eee262339d6946bcd	094be0aaf13d2b42d50dcc6418507b78
SHA256	121969d72f8e6f09ad93cf17500c479c452e230e27e7b157d5c9336dff15b6ef	05371b04e860f91503db9f81ff8b6451
Dominio	longlog[.]cc	N/A
Dominio	landim[.]cc	N/A
Dominio	hitchil[.]cc	N/A



[+ INFO](#)

ÚLTIMAS NOTICIAS

Ransomware en Azure

Microsoft interrumpió una campaña de ransomware Rhysida operada por el grupo Vanilla Tempest (Vice Society), que usaba binarios falsos de Microsoft Teams firmados con certificados digitales válidos, incluso del propio servicio de Trusted Signing de Azure. Los atacantes distribuían instaladores falsos de Teams desde dominios maliciosos creados mediante envenenamiento SEO, los cuales instalaban la puerta trasera Oyster para luego desplegar Rhysida. Microsoft revocó más de 200 certificados de firma de código usados para hacer pasar el malware como software legítimo. Las autoridades de certificación afirmaron estar investigando el posible uso indebido de certificados.

[+ INFO](#)

El malware de Android

Investigadores de Doctor Web descubrieron una nueva puerta trasera para Android llamada Android.Backdoor.Baohuo.1.origin, que se propaga mediante versiones falsas de Telegram X. El malware, distribuido a través de anuncios engañosos, se hace pasar por la app legítima y, tras la instalación, toma el control total de la cuenta de Telegram del usuario. Baohuo puede ocultar inicios de sesión no autorizados, borrar rastros de actividad y gestionar chats, canales y contactos sin que la víctima lo note, lo que la convierte en una de las amenazas más avanzadas de Android este año.

[+ INFO](#)

El malware RedTiger

RedTiger, una herramienta de código abierto basada en Python (originalmente para pruebas), fue adaptada por ciberdelincuentes. El malware inyecta código en Discord para robar tokens de autenticación de Discord, datos de pago guardados (tarjetas, PayPal), contraseñas del navegador, archivos de juegos, información de billeteras de criptomonedas, capturas de pantalla y fotos con la cámara. RedTiger incorpora anti-análisis (se apaga si detecta depuradores), usa "spam masivo de archivos y procesos" para entorpecer el análisis forense y tiene mecanismos de persistencia (funcional en Windows; parcial en Linux/macOS).

[+ INFO](#)

Un segundo para revisar puede evitar un gran problema

El phishing es una de las tácticas más comunes para engañar a las personas, si recibes un correo con solicitudes inusuales, como comprar tarjetas de regalo o realizar pagos urgentes, verifica siempre la identidad del remitente antes de actuar.

✔ Verifica siempre el remitente del correo: No te fíes solo del nombre visible; revisa la dirección completa. Un dominio extraño o mal escrito es una gran señal de alerta.

👤 Desconfía de solicitudes inusuales o urgentes: Siempre detente y confirma por otro canal oficial (teléfono, chat corporativo, etc.).

✉ Nunca compartas información sensible por correo: Las empresas legítimas nunca te pedirán datos personales, financieros ni contraseñas por e-mail.

📞 Revisa el tono y la redacción: Los mensajes falsos suelen tener errores gramaticales, saludos genéricos o un tono poco profesional.

🛡 Reporta inmediatamente los correos sospechosos: Usa el canal interno de seguridad o el equipo de TI para revisar el mensaje antes de tomar acción.

👉 Activa la autenticación multifactor (MFA): Aun si tus credenciales se filtran, este paso adicional puede evitar accesos no autorizados.

📌 Mantén una actitud vigilante: la prevención es la mejor defensa en ciberseguridad.





DataSec



CYBERSOC DTS



csirt_datasec@datasec.com.co



+57 310 315 9346 Ext. 4



© 2025 DataSec SAS. Todos los Derechos Reservados
CYBERSOC DTS by DataSec