Investigadores en ciberseguridad han revelado vulnerabilidades en ciertos modelos de cámaras web de Lenovo que podrían transformarlas en dispositivos de ataque tipo BadUSB.

"Esto permite que atacantes remotos inyecten pulsaciones de teclado de forma encubierta y ejecuten ataques independientemente del sistema operativo anfitrión", señalaron en un informe los investigadores de Eclypsium, Paul Asadoorian, Mickey Shkatov y Jesse Michael.

La compañía de seguridad de firmware ha denominado a estas fallas *BadCam*. Los hallazgos fueron presentados hoy durante la conferencia de seguridad DEF CON 33.

Este descubrimiento probablemente marque la primera ocasión en que se demuestra que actores maliciosos que obtienen control de un periférico USB basado en Linux, ya conectado a un equipo, pueden emplearlo con fines maliciosos.

En un escenario hipotético de ataque, un adversario podría aprovechar la vulnerabilidad para enviar a la víctima una cámara web con puerta trasera o conectarla al equipo si logra acceso físico, y posteriormente emitir comandos de manera remota para comprometer el sistema y ejecutar acciones posteriores a la intrusión.

BadUSB, demostrado por primera vez hace más de una década por los investigadores Karsten Nohl y Jakob Lell en la conferencia Black Hat 2014, es un tipo de ataque que explota una vulnerabilidad inherente al firmware USB, reprogramándolo para ejecutar comandos de manera discreta o correr programas maliciosos en la computadora de la víctima.

"A diferencia del malware tradicional, que reside en el sistema de archivos y puede ser detectado por herramientas antivirus, BadUSB se aloja en la capa de firmware", explica Ivanti en una descripción de la amenaza publicada a finales del mes pasado. *"Una vez conectado a un equipo, un dispositivo BadUSB puede: emular un teclado para introducir comandos maliciosos, instalar puertas traseras o registradores de teclas, redirigir el tráfico de internet y extraer información sensible"*.

En años recientes, Mandiant —propiedad de Google— y la Oficina Federal de Investigaciones

(FBI) de EE.UU. han advertido que el grupo de amenazas con motivación financiera identificado como FIN7 ha recurrido al envío de dispositivos USB maliciosos tipo *BadUSB* a organizaciones estadounidenses para distribuir un malware llamado DICELOADER.

Lenovo 510 FHD Webcam

Lenovo Performance FHD Webcam

El hallazgo más reciente de Eclypsium evidencia que un periférico USB, como cámaras web que ejecutan Linux, aun sin ser creado con intención maliciosa, puede convertirse en un vector para ataques BadUSB, representando una escalada notable. Se ha comprobado que estos dispositivos pueden ser secuestrados de forma remota y transformados en dispositivos BadUSB sin necesidad de desconectarlos o sustituirlos físicamente.

"Un atacante que obtenga ejecución remota de código en un sistema puede reescribir el firmware de una cámara web con Linux conectada, reconfigurándola para comportarse como un dispositivo HID malicioso o para emular dispositivos USB adicionales", explicaron los investigadores.

"Una vez armada, la aparentemente inofensiva cámara web puede inyectar pulsaciones de

teclado, entregar cargas maliciosas o servir como punto de persistencia profunda, todo mientras conserva la apariencia y funciones principales de una cámara común".

Además, los actores con capacidad de modificar el firmware de la cámara pueden lograr un mayor nivel de persistencia, permitiéndoles reinfectar el equipo incluso después de que haya sido formateado y el sistema operativo reinstalado.

Las vulnerabilidades encontradas en las cámaras Lenovo 510 FHD y Lenovo Performance FHD están relacionadas con la falta de validación del firmware, lo que las deja expuestas a un compromiso total del software de la cámara mediante ataques tipo BadUSB, dado que ejecutan Linux con soporte para USB Gadget.

Tras la divulgación responsable a Lenovo en abril de 2025, el fabricante de PC lanzó actualizaciones de firmware (versión 4.8.0) para mitigar las fallas y colaboró con la empresa china SigmaStar para desarrollar una herramienta que soluciona el problema.

"Este ataque, único en su tipo, expone un vector sutil pero profundamente problemático: los equipos, tanto empresariales como de consumo, suelen confiar en sus periféricos internos y externos, incluso cuando estos son capaces de ejecutar su propio sistema operativo y aceptar instrucciones remotas", dijo Eclypsium.

"En el caso de las cámaras web con Linux, el firmware sin firmar o con protección deficiente permite que un atacante comprometa no solo el sistema anfitrión, sino también cualquier otro equipo al que se conecte la cámara, propagando la infección y eludiendo los controles tradicionales".

Investigadores en ciberseguridad han revelado nuevos hallazgos sobre una vulnerabilidad ya corregida en el protocolo de comunicación Windows Remote Procedure Call (RPC) de Microsoft, la cual podría ser aprovechada por un atacante para realizar ataques de suplantación y hacerse pasar por un servidor legítimo.

El fallo, identificado como CVE-2025-49760 (con una puntuación CVSS de 3.5), fue descrito por la compañía tecnológica como un error de suplantación en Windows Storage. Se solucionó en julio de 2025 dentro de las actualizaciones mensuales del Patch Tuesday. Los detalles fueron expuestos por el investigador de SafeBreach, Ron Ben Yizhak, durante la conferencia de seguridad DEF CON 33 esta semana.

"El control externo del nombre o ruta de archivo en Windows Storage permite a un atacante autorizado realizar suplantación a través de la red", indicó la empresa en un aviso publicado el mes pasado.

El protocolo Windows RPC utiliza identificadores únicos universales (UUIDs) y un mapeador de puntos finales (Endpoint Mapper o EPM) para habilitar el uso de endpoints dinámicos en la comunicación cliente-servidor, conectando un cliente RPC con un endpoint registrado por un servidor.

La vulnerabilidad, en esencia, permite manipular un componente clave del protocolo RPC y llevar a cabo un ataque de envenenamiento de EPM, lo que posibilita que usuarios sin privilegios se hagan pasar por un servicio legítimo del sistema con el fin de forzar que un proceso protegido se autentique contra un servidor arbitrario controlado por el atacante.

Dado que el funcionamiento del EPM es similar al del Sistema de Nombres de Dominio (DNS) —mapeando un UUID de interfaz a un endpoint, del mismo modo que el DNS resuelve un dominio a una dirección IP—, el ataque se asemeja a un envenenamiento DNS, donde un actor malicioso altera los datos de DNS para redirigir a las víctimas a sitios web peligrosos.

Secuencia básica del ataque:

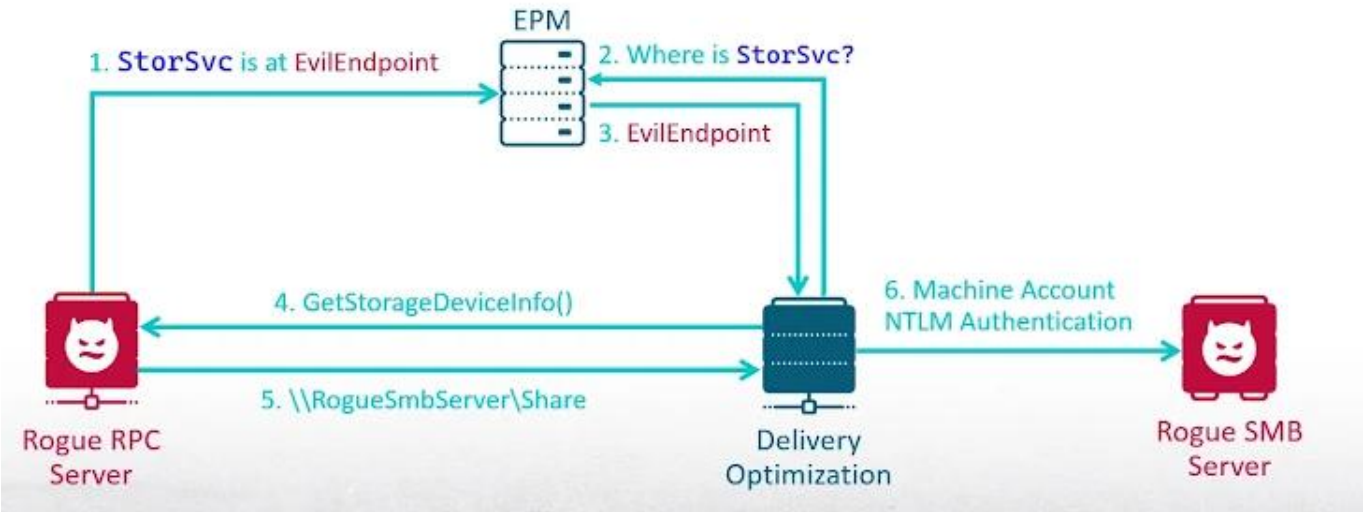
- Envenenar el EPM
- Hacerse pasar por un servidor RPC legítimo
- Manipular clientes RPC
- Escalar privilegios locales o de dominio mediante un ataque ESC8

"Me sorprendió descubrir que no había nada que impidiera registrar interfaces conocidas, integradas, que pertenecen a servicios esenciales", explicó Ben Yizhak en un informe compartido con The Hacker News. *"Esperaba, por ejemplo, que si Windows Defender tenía un identificador único, ningún otro proceso pudiera registrarlo. Pero no fue así"*.

"Cuando intenté registrar la interfaz de un servicio que estaba desactivado, su cliente se conectó a mí en su lugar. Este hallazgo fue increíble: el EPM no realizó ninguna verificación de seguridad. Conectó clientes a un proceso desconocido que ni siquiera se ejecutaba con privilegios de administrador".

El núcleo del ataque consiste en identificar interfaces que no estén asignadas a un endpoint, así como aquellas que puedan registrarse justo después de iniciar el sistema, aprovechando que muchos servicios están configurados con "inicio retrasado" para mejorar el rendimiento y acelerar el arranque.

En otras palabras, cualquier servicio con inicio manual representa un riesgo, ya que su interfaz RPC no se registrará al arrancar, lo que deja abierta la posibilidad de que un atacante se adelante y la registre antes que el servicio original.



SafeBreach también presentó una herramienta llamada RPC-Racer, diseñada para detectar servicios RPC inseguros (por ejemplo, Storage Service o StorSvc.dll) y manipular procesos Protected Process Light (PPL), como Delivery Optimization o DoSvc.dll, para que se autentiquen con una cuenta de máquina contra cualquier servidor definido por el atacante.

La tecnología PPL garantiza que el sistema operativo solo cargue servicios y procesos de confianza, protegiéndolos contra su terminación o infección por código malicioso. Microsoft la introdujo con Windows 8.1.

Resumen de la secuencia de ataque:

1. Crear una tarea programada para ejecutarse cuando el usuario actual inicie sesión
2. Registrar la interfaz del servicio Storage
3. Forzar que Delivery Optimization envíe una solicitud RPC a Storage, provocando que se conecte al endpoint dinámico del atacante
4. Invocar el método `GetStorageDeviceInfo()`, lo que lleva a que Delivery Optimization reciba un recurso SMB malicioso controlado por el atacante
5. Delivery Optimization se autentica en el servidor SMB con las credenciales de la cuenta de máquina, filtrando el hash NTLM
6. Realizar un ataque ESC8 para reenviar los hashes NTLM a los servicios web de inscripción de certificados (AD CS) y escalar privilegios

Para completar este ataque, puede utilizarse una herramienta ofensiva de código abierto como Certipy, la cual solicita un Ticket-Granting Ticket (TGT) de Kerberos usando un certificado generado a partir de la información NTLM obtenida, y posteriormente permite extraer todos los secretos del controlador de dominio.

SafeBreach advirtió que la técnica de envenenamiento EPM podría ampliarse para realizar ataques de *adversario-en-el-medio* (AitM) y de denegación de servicio (DoS), reenviando solicitudes al servicio original o registrando múltiples interfaces para bloquear las peticiones, respectivamente. La empresa también señaló que es probable que existan otros clientes e interfaces vulnerables a este tipo de ataque.

Para mejorar la detección, las soluciones de seguridad pueden monitorear llamadas a `RpcEpRegister` y emplear *Event Tracing for Windows* (ETW), una función que registra eventos generados por aplicaciones en modo usuario y controladores en modo kernel.

"Así como el SSL pinning verifica que un certificado no solo sea válido sino que use una clave pública específica, también debería comprobarse la identidad de un servidor RPC", afirmó Ben Yizhak.

"El diseño actual del endpoint mapper (EPM) no realiza esa verificación. Sin ella, los clientes aceptan datos de fuentes desconocidas. Confiar ciegamente en esa información permite a un atacante controlar las acciones del cliente y manipularlo a su antojo".

Investigadores en ciberseguridad han revelado una vulnerabilidad de alta gravedad en el editor de código impulsado por inteligencia artificial (IA) llamado Cursor, la cual podría permitir la ejecución remota de código.

La falla, identificada como CVE-2025-54136 (con una puntuación CVSS de 7.2), ha sido denominada *MCPoison* por Check Point Research, debido a que explota una peculiaridad en la forma en que el software gestiona las modificaciones en las configuraciones del servidor del Protocolo de Contexto de Modelo (MCP, por sus siglas en inglés).

"Una vulnerabilidad en Cursor AI permite a un atacante ejecutar código de forma remota y persistente al modificar un archivo de configuración MCP previamente confiable, ya sea dentro de un repositorio compartido de GitHub o editándolo localmente en la máquina de la víctima", indicó Cursor en un aviso publicado la semana pasada.

"Una vez que un colaborador aprueba un MCP aparentemente inofensivo, el atacante puede sustituirlo silenciosamente por un comando malicioso (por ejemplo, calc.exe) sin que se genere ninguna advertencia o solicitud adicional".

El MCP es un estándar abierto creado por Anthropic que permite a los modelos de lenguaje

de gran escala (LLMs) interactuar con herramientas externas, datos y servicios de manera uniforme. Fue introducido por la empresa en noviembre de 2024.

Según Check Point, la vulnerabilidad CVE-2025-54136 se relaciona con el hecho de que un atacante puede modificar el comportamiento de una configuración MCP después de que esta ha sido aprobada por el usuario en Cursor. El ataque se desarrolla de la siguiente forma:

- Agregar una configuración MCP aparentemente legítima (`.cursor/rules/mcp.json`) en un repositorio compartido
- Esperar a que la víctima descargue el código y lo apruebe una vez en Cursor
- Sustituir la configuración MCP por una carga maliciosa, como la ejecución de un script o una puerta trasera
- Lograr ejecución persistente de código cada vez que la víctima abra Cursor

El problema esencial es que, una vez que una configuración es aprobada, Cursor la considera confiable de forma indefinida, incluso si ha sido alterada. La explotación exitosa de esta falla no solo introduce riesgos en la cadena de suministro, sino que también permite el robo de datos e información confidencial sin que los usuarios lo adviertan.

Tras un proceso de divulgación responsable el 16 de julio de 2025, Cursor resolvió el problema en la versión 1.3, lanzada a finales de ese mes, exigiendo ahora una aprobación del usuario cada vez que se modifica una entrada en el archivo de configuración MCP.

"La falla revela una debilidad crítica en el modelo de confianza de los entornos de desarrollo asistidos por IA, elevando el nivel de riesgo para los equipos que integran LLMs y automatización en sus flujos de trabajo", señaló Check Point.

Este desarrollo se presenta pocos días después de que Aim Labs, Backslash Security y HiddenLayer revelaran múltiples debilidades en la herramienta de IA que podrían haber sido aprovechadas para ejecutar código de forma remota y evadir mecanismos de protección basados en listas de denegación. Estas también fueron corregidas en la versión 1.3.

Los hallazgos coinciden con la creciente adopción de la IA en procesos empresariales, incluyendo la generación de código mediante LLMs, lo cual amplía la superficie de ataque a nuevos riesgos como ataques a la cadena de suministro de IA, generación de código inseguro, envenenamiento de modelos, inyecciones de instrucciones (prompt injection), alucinaciones, respuestas inapropiadas y filtraciones de datos. Algunos ejemplos relevantes incluyen:

- Una prueba realizada a más de 100 LLMs sobre su capacidad para escribir código en Java, Python, C# y JavaScript reveló que el 45% de los fragmentos generados fallaban en pruebas de seguridad, introduciendo vulnerabilidades incluidas en el Top 10 de OWASP. Java lideró con un 72% de fallos, seguido por C# (45%), JavaScript (43%) y Python (38%).
- Un ataque denominado *LegalPwn* demostró que es posible usar textos legales, términos de servicio o políticas de privacidad como vectores de inyección de instrucciones, ocultando comandos maliciosos dentro de componentes legítimos pero poco vigilados, lo que puede hacer que el modelo clasifique código peligroso como seguro.
- El ataque *man-in-the-prompt* emplea una extensión maliciosa del navegador —sin permisos especiales— para abrir una nueva pestaña en segundo plano, iniciar un chatbot de IA e inyectar instrucciones dañinas para extraer información y comprometer la integridad del modelo. Esto se debe a que cualquier extensión con acceso al DOM puede interactuar directamente con las instrucciones del chatbot.
- La técnica de *jailbreak* llamada *Fallacy Failure* engaña al modelo con premisas lógicamente inválidas para inducirlo a generar respuestas restringidas, rompiendo sus propias reglas internas.
- *MAS hijacking* manipula el flujo de control en sistemas multiagente (MAS), permitiendo ejecutar código malicioso de manera transversal entre dominios, canales y topologías, aprovechando el comportamiento autónomo de los sistemas de IA.
- Una técnica conocida como *Poisoned GPT-Generated Unified Format (GGUF) Templates* ataca la fase de inferencia del modelo al incrustar instrucciones maliciosas dentro de archivos de plantilla de conversación. Al ejecutarse durante la inferencia, este enfoque logra evadir controles y pasar desapercibido. Dado que los archivos GGUF se

distribuyen a través de plataformas como Hugging Face, este ataque aprovecha la confianza en la cadena de suministro para activarse.
- También es posible comprometer los entornos de entrenamiento de aprendizaje automático como MLFlow, Amazon SageMaker o Azure ML, afectando la confidencialidad, integridad y disponibilidad de los modelos, lo cual puede derivar en movimientos laterales, escalación de privilegios y robo o envenenamiento de datos y modelos.
- Un estudio realizado por Anthropic reveló que los LLMs pueden adquirir características ocultas durante la destilación, un fenómeno llamado *aprendizaje subliminal*, que hace que los modelos transmitan comportamientos no deseados a través de datos generados, aunque parezcan no relacionados, lo que puede provocar desalineaciones y conductas dañinas.

"A medida que los modelos de lenguaje se integran profundamente en flujos de trabajo automatizados, copilotos empresariales y herramientas para desarrolladores, el riesgo asociado a estas técnicas de jailbreak se incrementa drásticamente", advirtió *Dor Sarig*, de Pillar Security. *"Los jailbreaks modernos pueden propagarse a través de cadenas contextuales, infectando un componente de IA y provocando fallos lógicos en cascada en sistemas interconectados"*.

"Estos ataques demuestran que la seguridad en IA requiere un enfoque completamente nuevo, ya que pueden eludir protecciones tradicionales sin depender de fallos estructurales o vulnerabilidades catalogadas. La debilidad radica en el propio lenguaje y razonamiento que los modelos están diseñados para imitar".

Google ha publicado actualizaciones de seguridad para corregir múltiples fallos en Android, entre ellos dos vulnerabilidades de Qualcomm que han sido *marcadas como explotadas activamente en entornos reales*.

Las fallas incluyen *CVE-2025-21479* (puntuación CVSS: 8.6) y *CVE-2025-27038* (puntuación CVSS: 7.5), ambas divulgadas junto con *CVE-2025-21480* (puntuación CVSS: 8.6) por el

fabricante de chips en junio de 2025.

CVE-2025-21479 corresponde a una vulnerabilidad de autorización incorrecta en el componente de Gráficos que podría provocar corrupción de memoria debido a la ejecución no autorizada de comandos en el microcódigo de la GPU.

Por su parte, *CVE-2025-27038* es una vulnerabilidad de tipo *use-after-free* en el mismo componente gráfico, que puede derivar en corrupción de memoria al renderizar gráficos mediante los controladores de GPU Adreno en Chrome.

Aún no se han revelado detalles sobre cómo se han utilizado estas vulnerabilidades en ataques reales, aunque Qualcomm indicó en su momento que *"hay indicios por parte del Grupo de Análisis de Amenazas de Google de que CVE-2025-21479, CVE-2025-21480 y CVE-2025-27038 podrían estar siendo explotadas de forma limitada y dirigida"*.

Dado que fallos similares en chips de Qualcomm han sido aprovechados anteriormente por proveedores de *spyware* comercial como Variston y Cy4Gate, se sospecha que estas vulnerabilidades también podrían haber sido explotadas en un contexto similar.

Las tres vulnerabilidades ya han sido incorporadas al catálogo de *Vulnerabilidades Conocidas y Explotadas (KEV)* de la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA), lo cual obliga a las agencias federales a aplicar los parches antes del 24 de junio de 2025.

El parche de agosto de 2025 de Google también corrige dos fallos de escalada de privilegios de alta gravedad en el Android Framework (*CVE-2025-22441* y *CVE-2025-48533*), así como una vulnerabilidad crítica en el componente del Sistema (*CVE-2025-48530*) que podría permitir la ejecución remota de código al combinarse con otros fallos, sin requerir permisos adicionales ni interacción del usuario.

El gigante tecnológico ha liberado dos niveles de parches, *2025-08-01* y *2025-08-05*, siendo este último el que también incluye correcciones para componentes de código cerrado y de

terceros, como los de Arm y Qualcomm. Se recomienda a los usuarios de dispositivos Android instalar estas actualizaciones tan pronto como estén disponibles para protegerse contra posibles amenazas.

Una combinación de métodos de propagación, narrativas sofisticadas y técnicas de evasión permitió que la táctica de ingeniería social conocida como ClickFix se expandiera con fuerza durante el último año, según nuevos hallazgos de Guardio Labs.

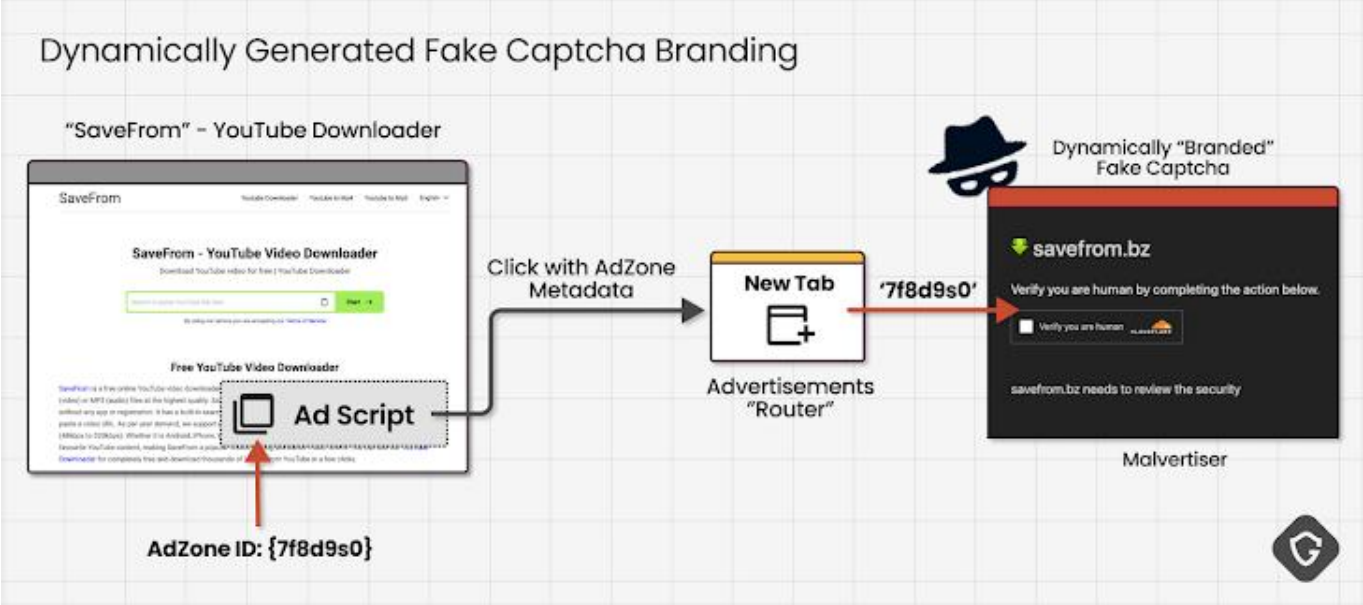
"Al igual que una variante viral en el mundo real, esta nueva cepa llamada 'ClickFix' superó rápidamente y terminó reemplazando por completo la infame estafa de falsas actualizaciones de navegador que dominaba la web el año pasado", señaló el investigador en ciberseguridad Shaked Chen en un informe.

"Lo logró eliminando la necesidad de descargas de archivos, utilizando tácticas de ingeniería social más inteligentes y aprovechando infraestructuras confiables para su distribución. El resultado: una oleada de infecciones que va desde ataques masivos tipo drive-by hasta campañas de spear-phishing altamente dirigidas."

ClickFix es el nombre atribuido a una técnica de engaño en la que las víctimas potenciales son inducidas a infectar sus propios equipos bajo la apariencia de resolver un problema inexistente o verificar un CAPTCHA. Su detección en entornos reales se remonta a principios de 2024.

En estos ataques se utilizan vectores de infección diversos como correos electrónicos de phishing, descargas silenciosas, malvertising y técnicas de envenenamiento SEO para redirigir a los usuarios hacia páginas falsas que muestran mensajes de error.

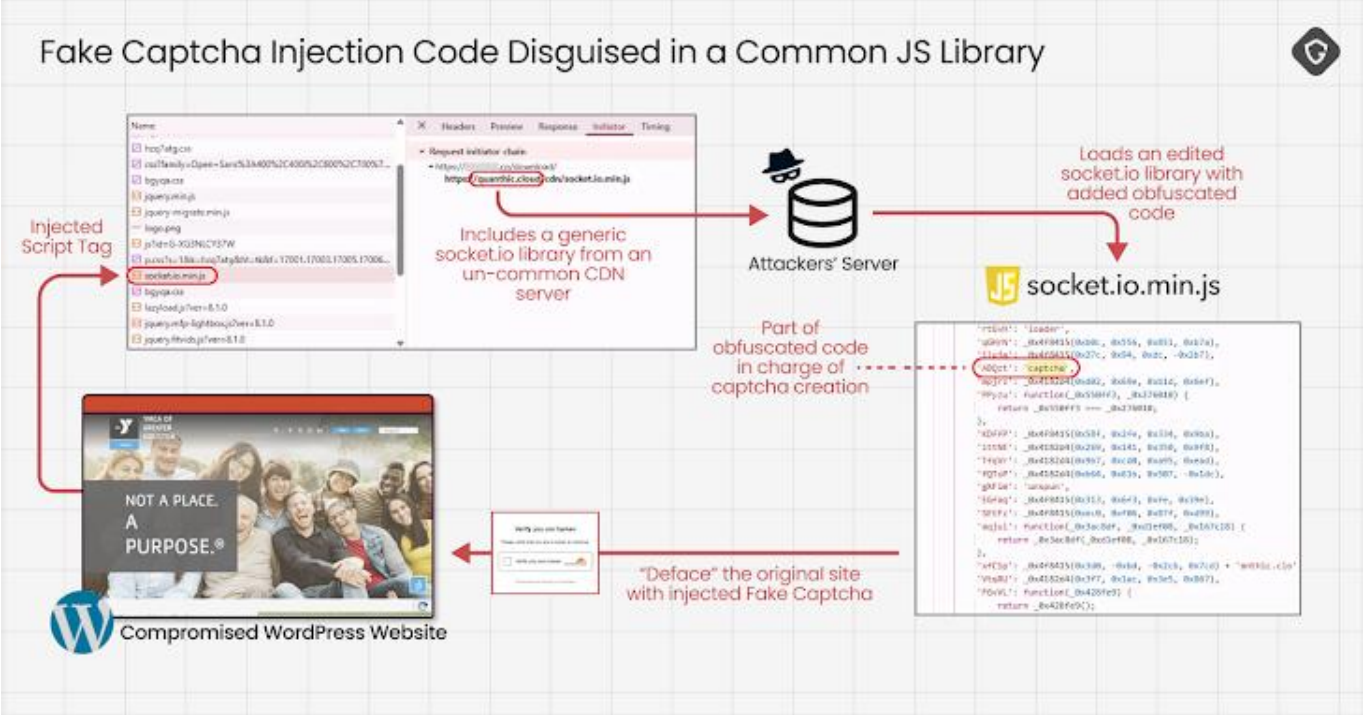
El propósito de estos mensajes es único: guiar a las víctimas a seguir una serie de pasos que terminan ejecutando un comando malicioso que fue copiado subrepticiamente al portapapeles, y que se activa al ser pegado en el cuadro de diálogo "Ejecutar" de Windows o en la app Terminal de macOS.



Este comando malicioso desencadena una cadena de ejecución por etapas, cuyo desenlace es la instalación de distintos tipos de malware como troyanos de acceso remoto (RAT), ladrones de información y cargadores, lo cual evidencia la versatilidad de la amenaza.

La táctica ha resultado tan eficaz y poderosa que ha derivado en lo que Guardio denomina un *CAPTCHAgeddon*, siendo utilizada tanto por cibercriminales como por actores estatales en decenas de campañas en un corto periodo de tiempo.

ClickFix representa una evolución más discreta de ClearFake, un método que se basa en sitios WordPress comprometidos para mostrar falsas actualizaciones de navegador que distribuyen malware tipo stealer. Posteriormente, ClearFake incorporó técnicas avanzadas de ocultamiento como EtherHiding, que utiliza contratos de la Binance Smart Chain (BSC) para esconder la carga maliciosa.



Guardio afirma que el éxito de ClickFix se debe a una mejora constante en sus vectores de propagación, la diversificación de los cebos y mensajes, y las múltiples formas de evadir los mecanismos de detección, al punto de haber reemplazado por completo a ClearFake.

"Los primeros mensajes eran genéricos, pero rápidamente se volvieron más convincentes, añadiendo elementos de urgencia o señales que despertaban sospechas", explicó Chen. *"Estos ajustes aumentaron la tasa de éxito al explotar presiones psicológicas básicas."*

Entre las adaptaciones más notables se encuentra el abuso de Google Scripts para alojar flujos falsos de CAPTCHA, aprovechando la confianza en los dominios de Google, así como la inserción de cargas maliciosas dentro de archivos que aparentan ser legítimos, como *socket.io.min.js*.

"Esta inquietante lista de técnicas – ofuscación, carga dinámica, archivos con apariencia legítima, compatibilidad multiplataforma, entrega de cargas por terceros y uso indebido de

dominios confiables como Google – demuestra cómo los atacantes han evolucionado constantemente para esquivar la detección”, añadió Chen.

“Es un recordatorio contundente de que estos actores no solo perfeccionan sus métodos de engaño, sino que invierten significativamente en técnicas técnicas para que sus ataques se mantengan efectivos y resistentes ante las medidas de seguridad.”

Investigadores en ciberseguridad han revelado una vulnerabilidad de alta gravedad ya corregida en Cursor, un popular editor de código impulsado por inteligencia artificial (IA), que podría permitir la ejecución remota de código (RCE).

El fallo, identificado como CVE-2025-54135 (con una puntuación CVSS de 8.6), fue solucionado en la versión 1.3 publicada el 29 de julio de 2025. Esta falla fue bautizada como *CurXecute* por Aim Labs, el mismo equipo que anteriormente dio a conocer *EchoLeak*.

“Cursor se ejecuta con privilegios de nivel desarrollador, y al vincularse con un servidor MCP que recolecta datos externos no confiables, esos datos pueden alterar el flujo de control del agente y explotar dichos privilegios”, explicó el equipo de Aim Labs.

“Al introducir datos manipulados al agente mediante MCP, un atacante puede lograr una ejecución remota de código completa bajo los privilegios del usuario, lo que permite desde ataques de ransomware y robo de datos, hasta manipulación y alucinaciones de la IA”.

En términos prácticos, la ejecución remota puede activarse mediante una única inyección de comandos hospedada externamente, que reescribe en silencio el archivo `~/.cursor/mcp.json` y ejecuta órdenes controladas por el atacante.

La vulnerabilidad guarda similitud con *EchoLeak*, ya que las herramientas expuestas por servidores MCP —utilizadas por los modelos de IA para interactuar con sistemas externos, como consultas a bases de datos o llamadas a APIs— pueden recibir datos no confiables que alteren el comportamiento esperado del agente.

Particularmente, Aim Security identificó que el archivo `mcp.json`, usado para configurar servidores MCP personalizados en Cursor, puede activar automáticamente cualquier entrada nueva (por ejemplo, añadir un servidor MCP de Slack) sin requerir confirmación.

Este modo de ejecución automática es especialmente peligroso, ya que permite la ejecución inmediata de una carga maliciosa inyectada por el atacante mediante un mensaje de Slack. La secuencia del ataque se desarrolla así:

1. El usuario añade un servidor MCP de Slack mediante la interfaz de Cursor.
2. El atacante publica un mensaje en un canal público de Slack con una carga de inyección de comandos.
3. La víctima abre un nuevo chat y solicita al agente de Cursor que resuma sus mensajes de Slack con una orden como: *"Utiliza herramientas de Slack para resumir mis mensajes"*.
4. El agente encuentra un mensaje diseñado para introducir comandos maliciosos, como modificar el archivo de configuración para añadir otro servidor MCP con instrucciones dañinas (por ejemplo, *«touch ~/<archivo_con_payload_RCE>»*).

"La raíz del problema es que las nuevas entradas en el archivo JSON global de MCP se ejecutan de forma automática", señaló Aim Security. *"Incluso si se rechaza la edición, la ejecución del código ya ocurrió"*.

Lo preocupante de este ataque es su simplicidad, pero también pone en evidencia cómo las herramientas asistidas por IA pueden abrir nuevas superficies de ataque al procesar contenido externo, como los servidores MCP de terceros.

"A medida que los agentes de IA conectan mundos externos, internos e interactivos, los modelos de seguridad deben asumir que los contextos externos pueden afectar la ejecución del agente — y es necesario monitorear cada paso", agregó la empresa.

La versión 1.3 de Cursor también aborda otro problema relacionado con el modo de ejecución automática, el cual puede eludir con facilidad los mecanismos de protección basados en

listas de denegación mediante técnicas como codificación en Base64, scripts de shell o comillas que disfrazan comandos peligrosos (por ejemplo, *«e»cho bypass»*).

Tras la divulgación responsable por parte del equipo de BackSlash Research, Cursor optó por eliminar por completo el uso de listas de denegación para la ejecución automática, adoptando en su lugar una lista de permitidos (allowlist).

"No hay que confiar ciegamente en las soluciones de seguridad integradas que ofrecen las plataformas de codificación con IA", afirmaron los investigadores Mustafa Naamneh y Micah Gold. *"La responsabilidad recae en las organizaciones usuarias para garantizar que los sistemas basados en agentes estén adecuadamente protegidos"*.

Esta revelación coincide con los hallazgos de HiddenLayer, que descubrió que la lista de denegación ineficaz de Cursor puede ser explotada al ocultar instrucciones maliciosas dentro de un archivo `README.md` en GitHub, lo que permite al atacante robar claves API, credenciales SSH e incluso ejecutar comandos prohibidos.

"Cuando la víctima visualizó el proyecto en GitHub, la inyección de comandos no era visible, y le pidió a Cursor que hiciera 'git clone' del proyecto y lo ayudara a configurarlo, algo común en sistemas IDE con agentes", detallaron los investigadores Kasimir Schulz, Kenneth Yeung y Tom Bonner.

"Pero al revisar el README para seguir las instrucciones, la inyección de comandos tomó el control del modelo de IA y lo obligó a usar la herramienta 'grep' para buscar claves en el espacio de trabajo del usuario, y luego exfiltrarlas con 'curl'".

HiddenLayer también identificó debilidades adicionales que permiten filtrar el prompt del sistema de Cursor al sobreescribir la URL base usada para las solicitudes a la API de OpenAI hacia un modelo con proxy, y exfiltrar claves SSH privadas del usuario combinando dos herramientas aparentemente inocuas: `read_file` y `create_diagram`, en lo que llamaron un "ataque de combinación de herramientas".

En esencia, esto consiste en insertar una inyección de comandos dentro del archivo `README.md` de GitHub, el cual Cursor analiza cuando el usuario le pide que resuma el archivo, ejecutando así el comando oculto.

La instrucción maliciosa utiliza `read_file` para acceder a las claves privadas SSH del usuario y luego emplea `create_diagram` para enviarlas a una URL controlada por el atacante en webhook.site. Todos estos fallos han sido corregidos por Cursor en la versión 1.3.

Estas noticias sobre vulnerabilidades en Cursor coinciden con un ataque diseñado por Tracebit contra *Gemini CLI*, una herramienta de línea de comandos de Google orientada a tareas de codificación, que aprovechaba una configuración por defecto para exfiltrar datos sensibles silenciosamente a un servidor del atacante mediante `curl`.

Al igual que en el caso de Cursor, el ataque requiere que la víctima (1) le pida a Gemini CLI interactuar con un repositorio de GitHub creado por el atacante que contiene una inyección indirecta en el archivo `GEMINI.md`, y (2) incluya un comando aparentemente inofensivo en una lista de permitidos, como `grep`.

"La inyección de comandos en estos elementos, combinada con serias deficiencias de validación y presentación dentro de Gemini CLI, puede dar lugar a ejecuciones de código arbitrarias indetectables", afirmó Sam Cox, fundador y CTO de Tracebit.

Para mitigar los riesgos, se recomienda a los usuarios de Gemini CLI actualizar a la versión 0.1.14, lanzada el 25 de julio de 2025.

Investigadores en ciberseguridad han identificado una puerta trasera en Linux, previamente no documentada, denominada Plague, la cual ha logrado eludir la detección durante un año.

"Este implante fue diseñado como un módulo malicioso PAM (Pluggable Authentication Module), lo que permite a los atacantes eludir discretamente la autenticación del sistema y mantener acceso persistente vía SSH", explicó Pierre-Henri Pezier, investigador de Nextron

Systems.

Los Módulos de Autenticación Enchufables (PAM, por sus siglas en inglés) son un conjunto de bibliotecas compartidas utilizadas para gestionar la autenticación de usuarios en aplicaciones y servicios dentro de sistemas Linux y UNIX.

Dado que estos módulos se cargan dentro de procesos de autenticación con privilegios elevados, un PAM malicioso puede permitir el robo de credenciales, eludir mecanismos de autenticación, y permanecer invisible a las herramientas de seguridad.

La firma de ciberseguridad informó que desde el 29 de julio de 2024, detectó múltiples muestras del malware Plague subidas a VirusTotal, ninguna de las cuales fue señalada como maliciosa por los motores antimalware. Además, la aparición de varias variantes indica que los actores detrás de esta amenaza continúan desarrollándola activamente.

Plague incorpora cuatro capacidades principales: el uso de credenciales estáticas para facilitar el acceso encubierto, mecanismos para evitar el análisis y la ingeniería inversa mediante técnicas anti-depuración y ofuscación de cadenas, y una mayor capacidad de sigilo mediante la eliminación de evidencias de sesiones SSH.

Esto se logra mediante la desactivación de variables de entorno como `SSH_CONNECTION` y `SSH_CLIENT` con el uso de `unsetenv`, así como redirigiendo `HISTFILE` a `/dev/null` para impedir el registro de comandos ejecutados en la terminal, con el objetivo de evitar cualquier rastro en los registros de auditoría.

"Plague se integra profundamente en la pila de autenticación, sobrevive a actualizaciones del sistema y apenas deja rastros forenses", destacó Pezier. *"Combinado con capas de ofuscación y manipulación del entorno, esto lo convierte en una amenaza sumamente difícil de identificar con herramientas convencionales"*.

El notorio grupo de ciberdelincuentes conocido como Scattered Spider está dirigiendo

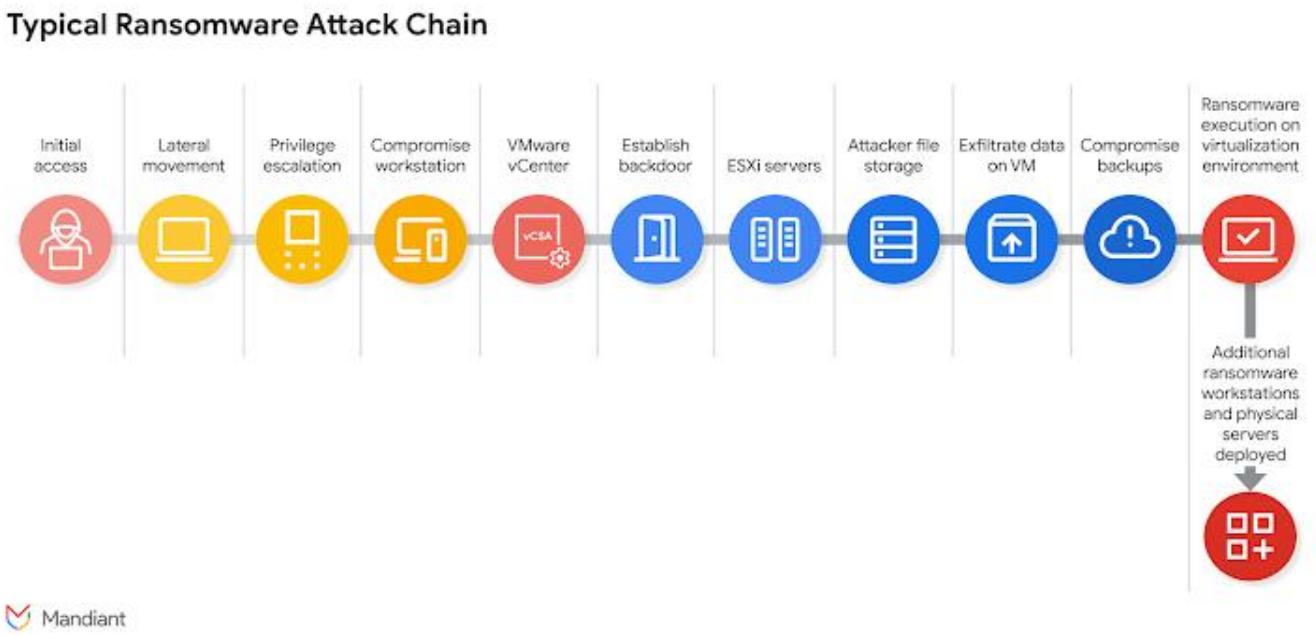
ataques contra hipervisores VMware ESXi, enfocándose en los sectores de comercio minorista, aerolíneas y transporte en América del Norte.

"Las tácticas principales del grupo se han mantenido constantes y no dependen de la explotación de vulnerabilidades en software. En su lugar, utilizan un método probado basado en llamadas telefónicas al servicio de asistencia técnica de TI", indicó el equipo de Mandiant de Google en un análisis detallado.

"Los actores son agresivos, ingeniosos y muestran una gran habilidad para emplear la ingeniería social con el fin de evadir incluso programas de seguridad maduros. Sus ataques no son aleatorios, sino campañas planificadas y dirigidas a los sistemas y datos más críticos de una organización."

También identificados como 0ktapus, Muddled Libra, Octo Tempest y UNC3944, estos actores de amenaza tienen un historial de ataques sofisticados mediante ingeniería social para obtener acceso inicial a los entornos de sus víctimas. Posteriormente, adoptan un enfoque de *"vivir de la tierra"* (*living-off-the-land*, LotL), manipulando sistemas administrativos confiables y aprovechando el control del Active Directory para acceder al entorno de VMware vSphere.

Google señaló que esta técnica, que permite la exfiltración de datos y el despliegue de ransomware directamente desde el hipervisor, es *"altamente efectiva"*, ya que evita las herramientas de seguridad y deja escasos rastros del compromiso.



La cadena de ataque se desarrolla en cinco fases distintas:

1. Compromiso inicial, reconocimiento y escalamiento de privilegios, permitiendo a los atacantes recopilar información relacionada con documentación de TI, manuales de soporte, organigramas y administradores de vSphere. También identifican credenciales almacenadas en gestores como HashiCorp Vault u otras soluciones de gestión de acceso privilegiado (PAM). Los atacantes suelen hacer llamadas adicionales al soporte técnico de la empresa, haciéndose pasar por administradores de alto nivel para solicitar el restablecimiento de contraseñas.
2. Acceso al entorno virtual mediante el uso de credenciales obtenidas de Active Directory para ingresar al VMware vCenter Server Appliance (vCSA). Luego ejecutan *teleport*, una herramienta que crea un shell inverso persistente y cifrado que evita las reglas del firewall.
3. Habilitación de conexiones SSH en los hosts ESXi, restablecimiento de contraseñas root, y ejecución de un ataque llamado *“disk-swap”* para extraer la base de datos NTDS.dit de Active Directory. Este ataque consiste en apagar una máquina virtual del

controlador de dominio (DC), desacoplar su disco virtual y conectarlo a otra VM no monitoreada bajo su control. Una vez copiado el archivo, el proceso se revierte y el DC se vuelve a encender.

4. Sabotaje del entorno de respaldo, eliminando tareas de copia de seguridad, instantáneas y repositorios para dificultar la recuperación.
5. Despliegue de ransomware, utilizando el acceso SSH a los hosts ESXi para transferir su binario personalizado mediante SCP o SFTP.

"El manual de operaciones de UNC3944 exige un cambio fundamental en la estrategia defensiva, pasando de la caza de amenazas basada en EDR a una defensa proactiva centrada en la infraestructura", señaló Google. *"Esta amenaza se diferencia del ransomware tradicional en entornos Windows en dos aspectos: velocidad y sigilo."*

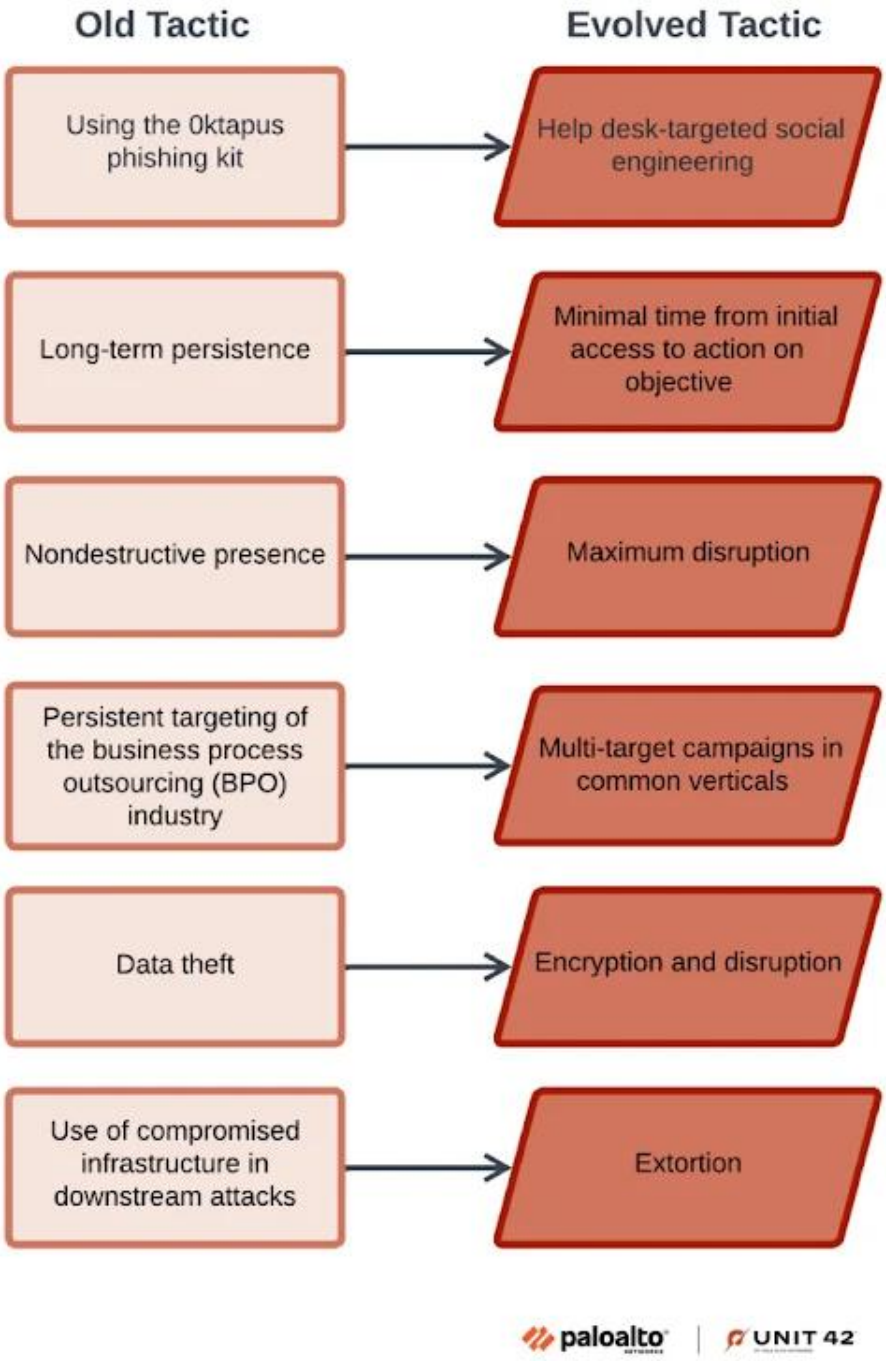
La empresa tecnológica también destacó la *"velocidad extrema"* del grupo, indicando que toda la secuencia, desde el acceso inicial hasta la exfiltración de datos y el despliegue final del ransomware, puede completarse en pocas horas.

De acuerdo con Unit 42 de Palo Alto Networks, los actores de Scattered Spider no solo han perfeccionado sus técnicas de ingeniería social, sino que también se han aliado con el grupo responsable del ransomware DragonForce (también conocido como *Slippery Scorpius*). En un caso, llegaron a exfiltrar más de 100 GB de datos en apenas dos días.

Para enfrentar estas amenazas, se recomienda implementar una estrategia de defensa en tres niveles:

- Activar el modo de bloqueo de vSphere, forzar el uso de *execInstalledOnly*, cifrar las máquinas virtuales, retirar VMs antiguas y reforzar el soporte técnico.
- Implementar autenticación multifactor resistente al *phishing*, aislar la infraestructura crítica de identidad y evitar bucles de autenticación.
- Centralizar y monitorear los registros clave, aislar las copias de seguridad del Active Directory en producción y asegurar que no sean accesibles para cuentas comprometidas.

Google también está instando a las organizaciones a rediseñar sus sistemas con un enfoque centrado en la seguridad, especialmente durante la transición desde VMware vSphere 7, cuya vida útil llegará a su fin en octubre de 2025.



"El ransomware dirigido a la infraestructura vSphere, que incluye tanto los hosts ESXi como el servidor vCenter, representa un riesgo excepcionalmente grave debido a su capacidad

para paralizar de inmediato y de forma generalizada toda la infraestructura," advirtió Google.

"No abordar de forma proactiva estos riesgos interconectados mediante la aplicación de las mitigaciones recomendadas dejará a las organizaciones vulnerables frente a ataques dirigidos, capaces de inutilizar rápidamente toda su infraestructura virtualizada, causando interrupciones operativas y pérdidas económicas."

Sophos y SonicWall han emitido alertas sobre fallos de seguridad críticos en Sophos Firewall y en los dispositivos Secure Mobile Access (SMA) de la serie 100, los cuales podrían ser aprovechados para ejecutar código de forma remota.

Los dos fallos que afectan a Sophos Firewall se describen a continuación:

- *CVE-2025-6704 (puntuación CVSS: 9.8)* – Una vulnerabilidad que permite escritura arbitraria de archivos en la función Secure PDF eXchange (SPX) podría permitir ejecución remota de código antes de la autenticación, si se utiliza una configuración específica de SPX junto con el firewall operando en modo de Alta Disponibilidad (HA).
- *CVE-2025-7624 (puntuación CVSS: 9.8)* – Una falla de inyección SQL en el antiguo proxy SMTP en modo transparente puede facilitar la ejecución remota de código si hay una política de cuarentena activa para correos electrónicos y el sistema fue actualizado desde una versión anterior a la 21.0 GA.

Sophos indicó que *CVE-2025-6704* afecta aproximadamente al 0.05% de los dispositivos, mientras que *CVE-2025-7624* impacta hasta el 0.73%. Ambas vulnerabilidades han sido corregidas junto con otra falla de alta gravedad, una inyección de comandos en el componente WebAdmin (*CVE-2025-7382*, *puntuación CVSS: 8.8*), que podría permitir la ejecución de código previa a la autenticación en dispositivos auxiliares bajo configuración HA, si la autenticación OTP está activada para el usuario administrador.

La empresa también solucionó otras dos vulnerabilidades:

- *CVE-2024-13974 (puntuación CVSS: 8.1)* – Una debilidad de lógica empresarial en el componente Up2Date que permitiría a un atacante manipular el entorno DNS del firewall y ejecutar código remotamente.
- *CVE-2024-13973 (puntuación CVSS: 6.8)* – Una vulnerabilidad de inyección SQL post-autenticación en WebAdmin que podría ser explotada por administradores para ejecutar código arbitrario.

El *Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC)* fue acreditado como descubridor y reportante tanto de *CVE-2024-13974* como de *CVE-2024-13973*. Las versiones afectadas son las siguientes:

- *CVE-2024-13974* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2024-13973* – Afecta a Sophos Firewall v21.0 GA (21.0.0) y anteriores
- *CVE-2025-6704* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7624* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores
- *CVE-2025-7382* – Afecta a Sophos Firewall v21.5 GA (21.5.0) y anteriores

La divulgación coincide con el informe de SonicWall sobre una vulnerabilidad crítica en la interfaz web de administración de la serie SMA 100 (*CVE-2025-40599, puntuación CVSS: 9.1*), que puede permitir a un atacante remoto con privilegios administrativos subir archivos arbitrarios y lograr ejecución remota de código.

Este fallo afecta a los productos SMA 100 Series (SMA 210, 410, 500v) y ya ha sido corregido en la versión 10.2.2.1-90sv.

SonicWall también señaló que, aunque no se ha detectado explotación activa, existe un riesgo potencial debido a un informe reciente del *Google Threat Intelligence Group (GTIG)*, el cual reveló que un actor de amenazas conocido como *UNC6148* ha utilizado dispositivos SMA 100 completamente actualizados para desplegar una puerta trasera llamada *OVERSTEP*.

Además de aplicar los parches disponibles, la compañía recomienda a los usuarios de dispositivos SMA 100 Series implementar las siguientes medidas:

- Deshabilitar el acceso de administración remota en la interfaz externa (X1) para reducir la superficie de ataque
- Restablecer todas las contraseñas y volver a vincular el OTP (One-Time Password) para usuarios y administradores del dispositivo
- Aplicar autenticación multifactor (MFA) para todos los usuarios
- Activar el Firewall de Aplicaciones Web (WAF) en los dispositivos SMA 100

También se aconseja a las organizaciones que revisen los registros del dispositivo y el historial de conexiones en busca de actividades sospechosas o accesos no autorizados.

En el caso del producto virtual *SMA 500v*, se requiere realizar una copia de seguridad del archivo OVA, exportar la configuración, eliminar la máquina virtual y todos sus discos y snapshots asociados, instalar nuevamente el OVA desde SonicWall usando un hipervisor y restaurar la configuración.

Cazadores de amenazas han revelado dos campañas de malware distintas que han explotado vulnerabilidades y configuraciones incorrectas en entornos en la nube con el objetivo de desplegar mineros de criptomonedas.

Los grupos de actividad maliciosa han sido identificados bajo los nombres de Soco404 y Koske por las firmas de seguridad en la nube Wiz y Aqua, respectivamente.

Soco404 "tiene como blanco sistemas tanto Linux como Windows, desplegando malware específico para cada plataforma", explicaron los investigadores de Wiz, Maor Dokhanian, Shahar Dorfman y Avigayil Mechtinger. *"Utilizan técnicas de suplantación de procesos para hacer pasar la actividad maliciosa como si fueran procesos legítimos del sistema."*

El nombre de la actividad hace alusión al hecho de que las cargas útiles están incrustadas en falsas páginas HTML con error 404, alojadas en sitios creados mediante Google Sites. Estos sitios fraudulentos ya fueron eliminados por Google.

Wiz señaló que esta campaña, anteriormente detectada atacando servicios Apache Tomcat con credenciales débiles, así como servidores vulnerables de Apache Struts y Atlassian Confluence a través del botnet Sysrv, parece formar parte de una infraestructura más amplia dedicada a fraudes con criptomonedas, incluyendo plataformas falsas de trading.

La campaña más reciente también ha apuntado a instancias PostgreSQL expuestas públicamente, y ha hecho uso de servidores Apache Tomcat comprometidos para alojar cargas útiles diseñadas para sistemas Linux y Windows. Además, los atacantes comprometieron un sitio legítimo de transporte surcoreano para distribuir el malware.

Una vez obtenida la entrada inicial, los atacantes aprovechan el comando SQL `COPY ... FROM PROGRAM` de PostgreSQL para ejecutar comandos shell arbitrarios en el sistema y obtener ejecución remota de código.

"El actor detrás de Soco404 parece llevar a cabo escaneos automatizados en busca de servicios expuestos, con la intención de explotar cualquier punto de entrada accesible", indicó Wiz. *"El uso de una amplia gama de herramientas de entrada, incluyendo utilidades de Linux como wget y curl, y herramientas nativas de Windows como certutil y PowerShell, demuestra una estrategia oportunista."*

En entornos Linux, se ejecuta directamente en memoria un script shell que actúa como dropper para descargar y lanzar la siguiente fase del ataque. Al mismo tiempo, elimina mineros competidores para maximizar beneficios y reduce la visibilidad forense sobrescribiendo registros relacionados con cron y wtmp.

La carga útil de esta segunda fase consiste en un binario que actúa como cargador del minero, contactando a un dominio externo (*www.fastsoco[.]top*), también basado en Google Sites.

En el caso de Windows, el ataque emplea un comando posterior a la explotación para descargar y ejecutar un binario de Windows, que funciona como su equivalente en Linux: un cargador que incluye tanto el minero como el controlador *WinRing0.sys*, utilizado para

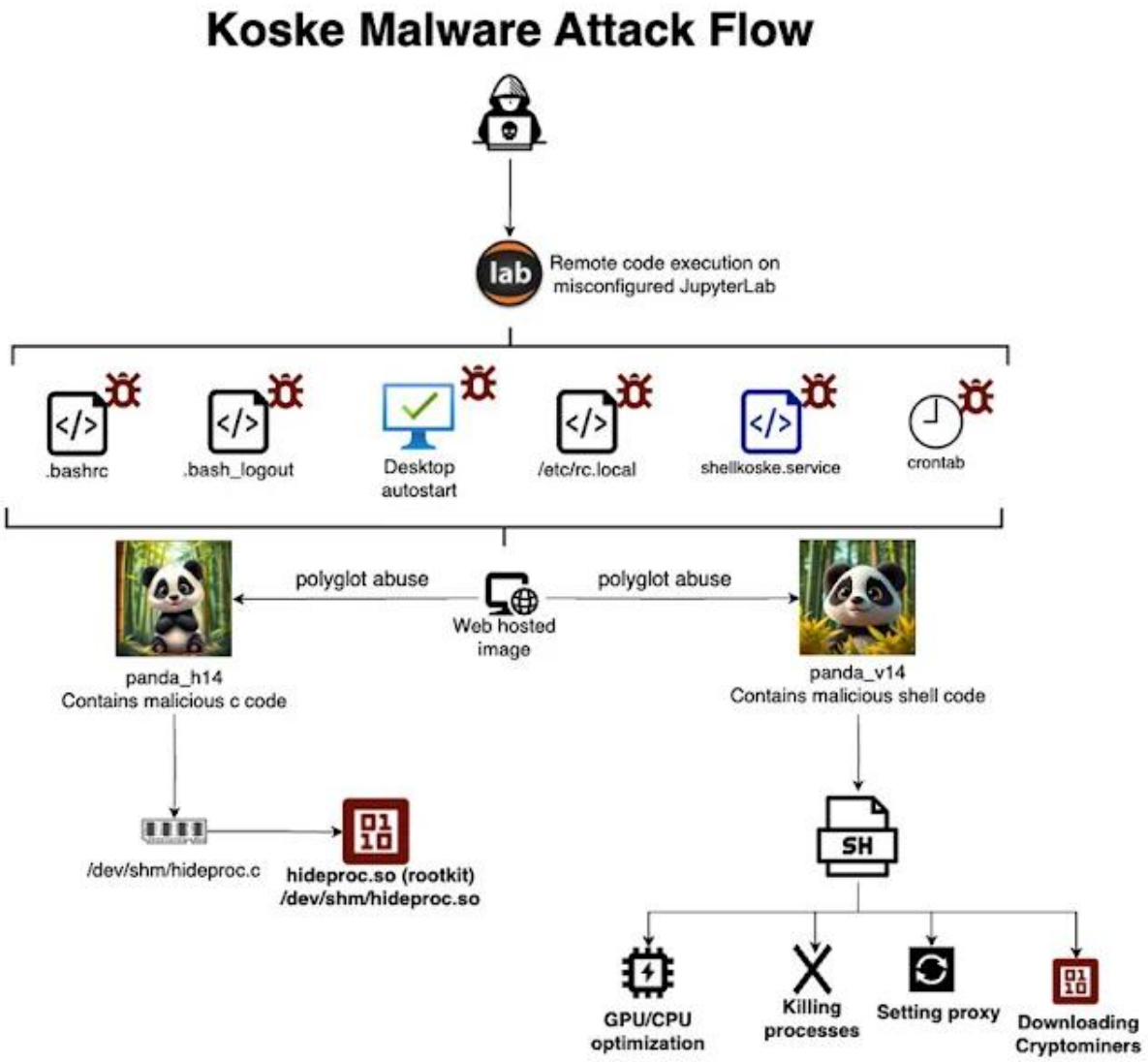
escalar privilegios hasta *NT\SYSTEM*.

Además, el malware intenta detener el servicio de registros de eventos de Windows y ejecuta un comando de autoeliminación para evitar ser detectado.

"En lugar de depender de un solo método o sistema operativo, el atacante lanza una red amplia, utilizando cualquier herramienta o técnica disponible en el entorno para desplegar su carga útil", señaló la empresa. *"Este enfoque flexible es característico de una campaña automatizada de criptominería diseñada para lograr el mayor alcance y persistencia posible en múltiples objetivos."*

El descubrimiento de Soco404 coincide con la aparición de una nueva amenaza para sistemas Linux denominada Koske, que se sospecha fue desarrollada con asistencia de un modelo de lenguaje de gran escala (LLM) y se propaga usando imágenes aparentemente inofensivas de pandas.

El ataque inicia con la explotación de un servidor mal configurado, como JupyterLab, para instalar varios scripts extraídos de dos imágenes JPEG. Entre estos se incluye un rootkit en C que oculta archivos relacionados con el malware utilizando *LD_PRELOAD* y un script shell que finalmente descarga los mineros de criptomonedas en el sistema comprometido. Ambas cargas se ejecutan directamente en memoria para evitar dejar rastros en el disco.



El objetivo final de Koske es desplegar mineros optimizados para CPU y GPU que utilicen los recursos del sistema para minar 18 criptomonedas diferentes, incluyendo Monero, Ravencoin, Zano, Nexa y Tari, entre otras.

“Estas imágenes son archivos poliglota, con cargas maliciosas añadidas al final. Una vez descargadas, el malware extrae y ejecuta los segmentos maliciosos en memoria, eludiendo

así los antivirus”, explicó el investigador de Aqua, Assaf Morag.

“Esta técnica no es esteganografía, sino un abuso de archivos poliglota o una forma de incrustación maliciosa. Se utiliza un archivo JPG válido al que se le añade shellcode malicioso al final. Solo se descargan y ejecutan los últimos bytes, lo que convierte esto en una forma sigilosa de abuso de archivos poliglota.”

When it comes to creating an outdoor space that combines style, durability, and sustainability, few materials rival high-density polyethylene, or HDPE. This synthetic resin has quickly become a favourite in the outdoor furniture market thanks to its impressive resistance to weather, insects, and fading. Whether you’re decorating a patio, decking out a poolside, or revamping a backyard retreat, selecting the best hdpe outdoor furniture a smart investment for long-lasting beauty and functionality.

Why Choose HDPE Furniture?
HDPE is a type of plastic made from recycled materials like milk jugs and detergent bottles, making it not only durable but also environmentally friendly. Unlike wood, HDPE does not rot, splinter, or require repainting. It’s impervious to moisture, resistant to UV rays, and doesn’t absorb heat like metal, making it incredibly comfortable in all climates from blistering summers to icy winters. This material is also virtually maintenance-free. A simple wipe-down with mild soap and water is usually enough to keep it looking brand new. With so many advantages, it’s no surprise that many homeowners are making the switch.

Features to Look for in the Best HDPE Outdoor Furniture

When shopping for the best hdpe outdoor furniture consider the following features:

- UV Resistance: Premium HDPE furniture includes UV inhibitors that prevent fading and preserve colour.
- Stainless Steel Hardware: Rust-resistant screws and bolts ensure the furniture holds up in wet or coastal environments.

- Ergonomic Design: Chairs and loungers should be designed with comfort in mind—curved backs, wide armrests, and generous seat depth.
- Stylish Options: Look for collections that come in a range of colors and styles to suit your outdoor décor.
- Assembly & Portability: Some pieces come pre-assembled, while others are flat-packed. Choose what suits your convenience and space.

Top Picks: Best HDPE Outdoor Furniture for All-Weather Comfort

Here's a curated list of standout HDPE furniture sets and pieces that deliver on comfort, style, and durability, making them ideal choices for any climate.

Foowin Classic Adirondack Chair

A staple in the HDPE furniture market, the Foowin Classic Adirondack Chair is timeless and practically built for all-weather living. It features a contoured seat, wide armrests, and a slanted back that invites you to kick back and relax. Available in a variety of colors, it's perfect for porches, decks, or fire pit circles.

Outer HDPE Outdoor Sofa Set

For those seeking plush best hdpe outdoor furniture Outer offers high-end modular furniture made with HDPE wicker and all-weather performance cushions. Their minimalist yet modern sofa sets are designed for comfort and engineered for the elements. The frame is built with HDPE lumber and resists cracking, warping, and fading.

Trex Outdoor Furniture Cape Cod 5-Piece Dining Set

Made from genuine HDPE lumber, Trex Outdoor Furniture offers eco-conscious dining options perfect for backyard meals or terrace brunches. The Cape Cod collection blends traditional style with lasting comfort. Chairs are ergonomically designed, and the table is spacious enough for family gatherings.

Highwood Weatherly Rocking Chair

The Highwood brand brings elegance and a hint of Southern charm with this HDPE rocking chair. Whether on the front porch or under a pergola, its gentle motion and weatherproof design make it a go-to for year-round relaxation.

LuxCraft Poly Lounge Set

For poolside lounging or sunny patios, the best hdpe outdoor furniture Poly Lounge Set delivers both aesthetics and functionality. Adjustable backs, wheels for easy movement, and optional cushions add to the experience.

Tips for Maximizing All-Weather Comfort

- Invest in Cushions: While HDPE is naturally comfortable, weather-resistant cushions can enhance seating, especially for extended use.
- Protect During Off-Season: Although HDPE is extremely durable, covering your furniture during prolonged periods of non-use can prolong its lifespan.
- Mix and Match: Many HDPE collections are modular. Pair a loveseat with individual chairs or a chaise lounge for a custom arrangement.
- Choose Neutral or Bold Colors: HDPE comes in a range of finishes—from crisp white and deep gray to tropical teal and sunflower yellow. Match your vibe or mix tones for added flair.

Final Thoughts

Choosing the is a decision that pays off season after season. Whether you want a cozy nook for reading or a spacious layout for entertaining, HDPE furniture offers the versatility and

resilience to meet your outdoor living needs. With minimal maintenance, eco-friendly appeal, and timeless good looks, HDPE furnishings are a top-tier choice for modern outdoor spaces.

Mitel ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en MiVoice MX-ONE que podría permitir a un atacante evadir los mecanismos de autenticación.

"Se ha detectado una falla de omisión de autenticación en el componente Provisioning Manager de Mitel MiVoice MX-ONE que, si es aprovechada exitosamente, permitiría a un atacante sin credenciales evadir los controles de acceso debido a una gestión inadecuada de permisos," señaló la empresa en un aviso emitido el miércoles.

"Una explotación exitosa de esta debilidad podría otorgar al atacante acceso no autorizado a cuentas de usuario o administrador dentro del sistema."

Esta vulnerabilidad, que aún no cuenta con un identificador CVE asignado, posee una puntuación CVSS de 9.4 sobre un máximo de 10. Afecta a las versiones de MiVoice MX-ONE desde la 7.3 (7.3.0.0.50) hasta la 7.8 SP1 (7.8.1.0.14).

Los parches correspondientes han sido distribuidos bajo los identificadores MXO-15711_78SP0 y MXO-15711_78SP1 para las versiones 7.8 y 7.8 SP1, respectivamente. Se recomienda a los clientes que utilicen MiVoice MX-ONE desde la versión 7.3 en adelante que soliciten el parche a su proveedor de servicios autorizado.

Como medidas de mitigación mientras se aplican las correcciones, se sugiere restringir la exposición directa de los servicios MX-ONE a internet y asegurarse de que operen dentro de una red de confianza.

Además de la falla de autenticación, Mitel también ha lanzado correcciones para una vulnerabilidad de alta gravedad en MiCollab (CVE-2025-52914, con una puntuación CVSS de 8.8) que podría permitir a un atacante autenticado ejecutar un ataque de inyección SQL.

“Una explotación exitosa de esta vulnerabilidad permitiría al atacante acceder a datos de aprovisionamiento de usuarios y ejecutar comandos SQL arbitrarios, lo cual comprometería la confidencialidad, integridad y disponibilidad del sistema,” indicó Mitel.

La vulnerabilidad afecta a las versiones de MiCollab desde la 10.0 (10.0.0.26) hasta la 10.0 SP1 FP1 (10.0.1.101), así como a la 9.8 SP3 (9.8.3.1) y versiones anteriores. El problema ha sido resuelto en las versiones 10.1 (10.1.0.10), 9.8 SP3 FP1 (9.8.3.103) y posteriores.

Dado el historial de ataques dirigidos a dispositivos Mitel, es crucial que los usuarios actualicen sus sistemas lo antes posible para reducir los riesgos de seguridad.