

GammaCS-C-CERT
By Gamma Ingenieros



Boletín de Ciberseguridad Semanal

Edición °3526



BOLETÍN DE CIBERSEGURIDAD SEMANTAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación, tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y para nuestros aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	3	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

SERVICENOW AI PLATFORM Y NOW PLATFORM – MÚLTIPLES VULNERABILIDADES CRÍTICAS PERMITEN EJECUCIÓN REMOTA DE CÓDIGO, ESCALADA DE PRIVILEGIOS E INYECCIÓN SQL (CVE-2026-18885 / CVE-2026-18886 / CVE-2026-74820 / CVE-2026-6876)

ServiceNow ha publicado un aviso de seguridad urgente (KB3152242) para corregir cuatro vulnerabilidades en sus plataformas ServiceNow AI Platform y Now Platform. Tres de estos fallos alcanzan la máxima puntuación de severidad (CVSS 10.0) y permiten a atacantes remotos no autenticados ejecutar código arbitrario, escalar privilegios o ejecutar sentencias SQL arbitrarias contra la base de datos subyacente de la instancia. La cuarta vulnerabilidad corresponde a un escape de sandbox de severidad alta (CVSS 8.7). Dado que la mayoría de los vectores de ataque no requieren credenciales ni interacción del usuario, la exposición representa un riesgo crítico para las operaciones corporativas.

Resumen técnico:

- Identificador principal: CVE-2026-18885, CVE-2026-18886, CVE-2026-74820 y CVE-2026-6876.
- Severidad: Crítica (CVSS v4.0: 10.0 para CVE-2026-18885, CVE-2026-18886 y CVE-2026-74820; CVSS v4.0: 8.7 / Alta para CVE-2026-6876 / Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).
- Causa raíz: Inyección de código en API GraphQL (CWE-94), control de acceso inadecuado en el procesador de carga de imágenes (CWE-284), inyección SQL mediante cláusulas ORDER BY dinámicas (CWE-89) y escape del sandbox en el entorno de ejecución.
- Mecanismo de falla:
- CVE-2026-18885: Una falla de inyección de código en la API GraphQL Composite Data permite a un atacante no autenticado ejecutar comandos del sistema y modificar datos de la instancia.
- CVE-2026-18886: Una falta de validación de límites de autorización en el procesador de carga de imágenes de configuración del sistema faculta a usuarios no autenticados a crear o alterar datos de la instancia, logrando una escalada de privilegios.
- CVE-2026-74820: Una vulnerabilidad de inyección SQL en la construcción de la cláusula ORDER BY del esquema dinámico permite la ejecución arbitraria de consultas SQL contra la base de datos de la plataforma.
- CVE-2026-6876: Un fallo de escape de sandbox en la plataforma Now permite a usuarios ejecutar código arbitrario dentro del entorno restringido de la plataforma.
- Estado de explotación: Divulgadas oficialmente por ServiceNow el 27 de agosto de 2026. El fabricante no registra evidencia de explotación activa ni código de explotación público a la fecha; sin embargo, CISA ha clasificado los fallos con severidad 10.0 como automatizables a escala de Internet.
- Versiones afectadas: Instancias de ServiceNow en las familias de versiones Xanadu (anteriores a Patch 11 Hot Fix 7a), Yokohama (anteriores a Patch 12 Hot Fix 3b y Patch 13 Hot Fix 4), Zurich (anteriores a Patch 7b Hot Fix 3, Patch 8 Hot Fix 5, Patch 9 Hot Fix 6, Patch 10 Hot Fix 2m/3, Patch 11 y Patch 12) y Australia (anteriores a Patch 2 Hot Fix 3, Patch 3 Hot Fix 2, Patch 3m, Patch 4 y Patch 5).

Impacto potencial:

- Ejecución remota de código y control de la plataforma: Permite a atacantes anónimos ejecutar código arbitrario con privilegios en la infraestructura de la plataforma, sirviendo como punto de apoyo para comprometer el entorno operativo.
- Exfiltración masiva de datos e información confidencial: Mediante la inyección SQL (CVE-2026-74820), los atacantes pueden consultar directamente la base de datos subyacente, exponiendo inventarios de la CMDB, credenciales almacenadas en tickets de soporte, registros de recursos humanos y datos de TI.
- Escalada de privilegios y alteración de registros del sistema: El fallo de control de acceso (CVE-2026-18886) permite la creación y modificación no autorizada de datos, otorgando capacidades administrativas completas a usuarios no autenticados.
- Efecto de amplificación en workflows de IA y movimiento lateral: La interconexión de la plataforma ServiceNow con agentes de IA y sistemas corporativos expone llaves de integración y tokens de autenticación, permitiendo al atacante pivotar hacia otros activos clave de la organización.

Recomendaciones de mitigación:

1. Aplicación prioritaria de parches de seguridad: Desplegar inmediatamente las actualizaciones y parches de hotfix oficiales según la rama de versión correspondiente (Xanadu, Yokohama, Zurich o Australia). En entornos SaaS, verificar que la actualización automática haya sido aplicada correctamente.
2. Restricción de rutas de carga de imágenes no autenticadas: Deshabilitar o bloquear temporalmente las interfaces públicas de carga de archivos e imágenes de configuración mientras se completa el proceso de parcheo.
3. Monitoreo y auditoría activa de registros: Configurar reglas de detección e inspección en el SIEM/WAF para identificar peticiones GraphQL anómalas desde sesiones anónimas, cargas de imágenes no autorizadas y construcciones de consultas SQL inusuales con cláusulas ORDER BY.
4. Aislamiento perimetral y rotación de credenciales de integración: Restringir el acceso a la plataforma únicamente a rangos de IP de confianza mediante listas de control de acceso (ACLs) y proceder con la rotación de claves API, tokens y credenciales de integración almacenadas en la instancia.

Prioridad: Crítica.

Ampliar información:

- <https://thehackernews.com/2026/08/three-cvss-100-servicenow-flaws-could.html>
- <https://www.pk-sharma.com/briefing/servicenow-three-cvss-10-unauthenticated-flaws>
- <https://tech.yahoo.com/cybersecurity/articles/three-cvss-10-0-vulnerabilities-022149856.html>
- <https://kudelskisecurity.com/research/three-critical-servicenow-platform-vulnerabilities-could-allow-arbitrary-execution-privilege-escalation>
- <https://breached.company/servicenow-three-cvss-10-unauthenticated-rce-sql-injection-2026/>

ROUTERS ZBTLINK / ZBT – IMPLANTES Y PUERTAS TRASERAS DE FÁBRICA PERMITEN EJECUCIÓN REMOTA DE CÓDIGO CON PRIVILEGIOS DE ROOT Y ESPIONAJE SIN AUTENTICACIÓN (CVE-2026-74232 / CVE-2026-74233)

Investigadores de seguridad de la firma Vulncheck han revelado la presencia de dos implantes de fábrica no documentados (denominados SPEAKINGSTONE y DARKLANTERN) en el firmware de routers fabricados por la empresa china Shenzhen Zhibotong Electronics (ZBT / Zbtlink). Estas puertas traseras permiten a atacantes remotos no autenticados ejecutar comandos arbitrarios con privilegios de superusuario (root), exfiltrar credenciales de acceso a internet del proveedor (PPPoE) y realizar secuestro de consultas DNS. Debido a que los implantes se encuentran integrados intencionalmente en el firmware de fábrica y el fabricante afirma que corresponden a herramientas de soporte técnico, no se dispone de parches oficiales al momento de la publicación.

Resumen técnico:

- Identificador principal: CVE-2026-74232 (SPEAKINGSTONE) y CVE-2026-74233 (DARKLANTERN).
- Severidad: Crítica (CVSS v3.1: 9.8 / CVSS v4.0: 9.3 / Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Inserción intencional de implantes en el firmware de fábrica, comandos no sanitizados (CWE-77/78), omisión de mecanismos de autenticación mediante valores comodín y uso de claves de cifrado estáticas.
- Mecanismo de falla:
- DARKLANTERN (CVE-2026-74233): Opera mediante el servicio infosrvd en el puerto UDP 9992, expuesto públicamente por el firewall predeterminado del router. Permite ejecutar comandos remotamente en /etc/exec/cmd con privilegios de root, evadiendo la validación de dirección MAC mediante la cadena comodín (00:00:00:00:00:00) y un hash estático generado con la clave hardcodeda mqonu.com.SPEAKINGSTONE
- (CVE-2026-74232): Ejecutado como el servicio yunmgrd, envía beacons salientes por UDP 10000 hacia la infraestructura C2 (ac-link.com o findmyipaddr.com). El protocolo no autenticado zbtProtocol permite ejecutar comandos remotos, exfiltrar usuarios y contraseñas WAN PPPoE, modificar listas de redirección DNS y establecer túneles SSH reversos, incluso cuando el equipo está detrás de firewall o NAT.
- Estado de explotación: Divulgados públicamente entre el 27 y el 28 de agosto de 2026 por VulnCheck. Se registran cientos de dispositivos expuestos en internet respondiendo a escaneos entrantes y realizando beaconing saliente de forma activa.
- Versiones / Modelos afectados: Múltiples modelos y versiones de firmware de routers ZBT / Zbtlink (tales como WE826-T2, WE1326, WE357, WE5926, WG3526, L3_V2_8, ZBT-7628, entre otros), así como marcas blancas o distribuidores que reempaquetan el hardware y firmware de ZBT (incluyendo Deep Orange, WiFlyer, Cioswi, CroSkylink, MoreQuick, KuWFi, OneX, Digineo y ALLNET).

Impacto potencial:

- Ejecución remota de comandos con privilegios de root: Un atacante puede tomar control total del dispositivo ejecutando instrucciones arbitrarias del sistema operativo sin requerir credenciales ni interacción del usuario.
- Exfiltración de credenciales sensibles de acceso a Internet: Permite la extracción no autorizada de nombres de usuario y contraseñas del protocolo WAN PPPoE almacenados en el router.
- Secuestro de tráfico mediante manipulación de DNS (DNS Hijacking): Faculta a los atacantes a alterar las tablas de resolución DNS del router para redirigir el tráfico de los usuarios locales hacia sitios maliciosos o de suplantación de identidad.
- Intercepción y movimiento lateral mediante túneles SSH reversos: Habilita la apertura de túneles SSH salientes, lo que permite evadir cortafuegos perimetrales y establecer un punto de acceso directo a la red interna corporativa o residencial.

Recomendaciones de mitigación:

1. Reemplazo prioritario de dispositivos afectados: Dado que se trata de implantes intencionales en el firmware y no existe un parche oficial disponible, se recomienda retirar y sustituir los routers ZBT/Zbtlink o de marcas blancas derivadas por equipos de fabricantes confiables.
2. Bloqueo perimetral de dominios y puertos de comunicación: Configurar reglas en los cortafuegos para bloquear el tráfico saliente hacia los dominios C2 conocidos (ac-link.com y findmyipaddr.com), así como denegar el tráfico en los puertos UDP 9992 (entrante) y UDP 10000 (saliente).
3. Identificación de hardware de marca blanca mediante prefijos MAC: Auditar los dispositivos de red e identificar equipos cuyo prefijo de dirección MAC corresponda a los bloques asignados a Shenzhen Zhibotong Electronics (78:A3:51 y F8:5E:3C).
4. Aislamiento y segmentación estricta de la red: En caso de no poder retirar los equipos de forma inmediata, aislar los routers en una VLAN sin acceso a activos críticos de la organización y tratar el segmento LAN correspondiente como no confiable.

Prioridad: Crítica.

Ampliar información:

- <https://thehackernews.com/2026/08/china-made-zbt-routers-ship-with-two.html>
- <https://www.vulncheck.com/blog/zbt-darklantern-speakingstone>
- <https://www.heise.de/en/news/OEM-China-routers-from-ZBT-with-backdoors-11433363.html>
- <https://www.pcmag.com/news/more-wi-fi-routers-from-this-chinese-vendor-found-with-backdoors>
- <https://www.privacyguides.org/news/2026/08/31/router-manufacturer-found-with-multiple-backdoors-in-its-products/>

CPANEL Y WHM – VULNERABILIDAD EN GESTIÓN DE DOMINIOS PARQUEADOS Y ADICIONALES PERMITE CREACIÓN ARBITRARIA DE ARCHIVOS Y ESCALADA DE PRIVILEGIOS A ROOT (CVE-2026-65643)

cPanel ha publicado un aviso de seguridad crítico para corregir la vulnerabilidad CVE-2026-65643, la cual afecta a todas las versiones con soporte del panel de control cPanel & WHM. El fallo radica en la funcionalidad de dominios parqueados (parked domains) y adicionales (addon domains), permitiendo a un usuario autenticado con permisos básicos crear archivos arbitrarios en cualquier ruta del sistema de archivos del servidor. La explotación exitosa deriva en la ejecución remota de código con privilegios de superusuario (root), otorgando control total de la infraestructura compartida, así como de las cuentas, sitios web y bases de datos alojadas en la máquina.

Resumen técnico:

- Identificador principal: CVE-2026-65643.
- Severidad: Alta / Crítica (CVSS v4.0: 8.7 / Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H / Clasificado como Crítico por el fabricante).
- Causa raíz: Sanitización e inspección insuficiente de entradas en la generación de archivos de configuración para dominios adicionales y parqueados (Creación arbitraria de archivos / CWE-22).
- Mecanismo de falla: Un usuario autenticado con permisos para agregar dominios adicionales o parqueados envía solicitudes manipuladas durante el registro del dominio. El panel procesa la solicitud y genera archivos fuera del directorio permitido del cliente, depositando un archivo ejecutable en ubicaciones privilegiadas del sistema que posteriormente es ejecutado con privilegios de superusuario (root).
- Estado de explotación: Divulgada oficialmente el 27 de agosto de 2026 por cPanel tras el hallazgo del investigador Devon Courtney. No se registra evidencia de explotación activa masiva en el entorno real ni inclusión en el catálogo KEV de CISA al momento de la publicación.
- Versiones afectadas: Todas las versiones soportadas de cPanel/WHM anteriores a las compilaciones corregidas: rama 11.110 (anteriores a 11.110.0.141), rama 11.134 (anteriores a 11.134.0.53), rama 11.136 (anteriores a 11.136.0.37), rama 11.138 (anteriores a 11.138.0.2) y la compilación WP Squared (anteriores a 11.138.1.7).

Impacto potencial:

- Escalación total de privilegios a nivel de superusuario (root): Un usuario con una cuenta básica de alojamiento web puede vulnerar el aislamiento del entorno multi-inquilino y obtener privilegios de administración absoluta sobre el servidor anfitrión.
- Compromiso integral de entornos de alojamiento compartido (Shared Hosting): Al obtener acceso de superusuario, el atacante puede acceder, alterar o eliminar de forma no autorizada los sitios web, archivos de configuración, bases de datos y buzones de correo de todos los demás clientes alojados en el mismo servidor.
- Exfiltración masiva de datos e información confidencial: Faculta la extracción de credenciales de bases de datos, claves de cifrado, secretos de aplicaciones y datos personales procesados por las plataformas web alojadas en la infraestructura.
- Despliegue de persistencia y movimiento lateral en la red corporativa: El atacante puede instalar lazos de persistencia (como tareas programadas maliciosas o puertas traseras) e intentar pivotar hacia otros segmentos de la red del proveedor de servicios de alojamiento.

Recomendaciones de mitigación:

1. Actualización prioritaria a compilaciones corregidas: Ejecutar la actualización inmediata de cPanel/WHM en los servidores afectados hacia las versiones seguras (11.110.0.141, 11.134.0.53, 11.136.0.37, 11.138.0.2 o 11.138.1.7 en adelante) mediante los scripts de actualización del sistema o desde la consola de administración.
2. Restricción temporal de características de gestión de dominios: En caso de no poder aplicar la actualización inmediatamente, restringir o deshabilitar temporalmente la capacidad de agregar dominios parqueados y adicionales a través de las listas de características en la interfaz de administración.
3. Auditoría e inspección de integridad del sistema de archivos: Revisar archivos del sistema modificados recientemente en rutas privilegiadas, la presencia de tareas programadas (cron jobs) no autorizadas y cuentas creadas con privilegios anómalos.
4. Monitoreo de registros de acceso y eventos del servidor: Auditar los registros de solicitudes web de la plataforma de administración en busca de patrones atípicos de registro de dominios o intentos de manipulación de rutas de archivos.

Prioridad: Crítica.

Ampliar información:

- <https://support.cpanel.net/hc/en-us/articles/42959571221527-Security-CVE-2026-65643-Vulnerability-in-cPanel-s-Domain-Parking-Functionality-August-27-2026>
- <https://thehackernews.com/2026/08/critical-cpanel-flaw-could-let-one.html>
- <https://devel.group/blog/vulnerabilidad-critica-en-cpanel-permite-toma-de-control-root-cve-2026-65643/>
- <https://pasqualepillitteri.it/en/news/13179/cpanel-cve-2026-65643-root-server>
- <https://rdd.com.do/blog/vulnerabilidad-cpanel-cve-2026-65643-control-servidor>

MALWARE

STREAMRAT – TROYANO BANCARIO Y INFOSTEALER PARA ANDROID SE DISTRIBUYE VÍA ANUNCIOS MALICIOSOS EN META Y TIKTOK MEDIANTE FALSAS APLICACIONES DE STREAMING

Investigadores de ciberseguridad han detectado una campaña de anuncios maliciosos (malvertising) en plataformas de Meta (Facebook e Instagram) y TikTok que distribuye un nuevo troyano bancario e infostealer para Android denominado StreamRat. Dirigida principalmente a usuarios de habla hispana, la campaña utiliza como señuelo la promesa de acceso gratuito a plataformas de televisión en vivo. Una vez instalado en el dispositivo objetivo, el malware permite a los atacantes obtener un control casi total sobre la unidad infectada, interceptar credenciales bancarias y ejecutar acciones remotas sin el conocimiento de la víctima.

Resumen técnico:

- Identificador principal: Troyano bancario y de control remoto StreamRat para Android (Hashes SHA-256: e0714788b4e2518b0d9d4cbf18c7217bb97718e01689d77338f1cc4a230fcb6c / Nombres de paquete: io.base.one887, io.meat.hint).
- Tipo de amenaza: Troyano bancario (Banking Trojan), Extractor de información (Infostealer), Herramienta de control remoto (VNC/HVNC) y Dropper malicioso.
- Mecanismo de acceso e infección: La cadena de infección inicia con anuncios en redes sociales que dirigen a sitios web de phishing adaptativos. Si se detecta un sistema Android, el sitio despliega instrucciones detalladas para guiar al usuario a habilitar la instalación de aplicaciones desde fuentes desconocidas (sideloading) e instalar un archivo APK disfrazado de reproductor de TV (por ejemplo, "StreamTV Pro" o "Sistema de vídeo").
- Capacidades avanzadas y evasión:
- Interrupción de telemetría de seguridad: El dropper solicita permisos para establecer un túnel VPN ficticio que redirige y bloquea el tráfico de red de otras aplicaciones, impidiendo que soluciones de seguridad o servicios como Google Play Protect realicen análisis de reputación en la nube durante la instalación.
- Captura de pantalla discreta (VNC/HVNC): Dispone de un modo VNC mediante la API MediaProjection y un modo VNC oculto (HVNC) utilizando la API de Accesibilidad para capturar capturas de pantalla cada 200 milisegundos sin indicadores visibles.
- Pantallas de distracción: Puede bloquear la pantalla con una portada negra o una simulación de "actualización del sistema" para ocultar la actividad del atacante en segundo plano.
- Canales y transportes soportados: Establece comunicación con su servidor de comando y control (C2) mediante protocolos WebSocket personalizados utilizando cabeceras HTTP modificadas. Descarga la carga útil final desde repositorios públicos como GitHub y transmite datos comprimidos en formato WebP e inspecciones de la interfaz en objetos JSON.

- Mecanismos de persistencia y abuso de privilegios: Solicita convertirse en la aplicación de inicio predeterminada (launcher) para recuperar el control cuando la víctima presiona el botón Inicio, y abusa extensivamente de los Servicios de Accesibilidad de Android (Accessibility Services) para inspeccionar la jerarquía de la pantalla (UI Tree), capturar pulsaciones de teclado (keylogging) y superponer pantallas falsas (overlays).
- Estado de actividad: Campaña activa reportada a inicios de septiembre de 2026 con un alcance estimado de más de 570.000 cuentas expuestas en la Unión Europea.

Impacto potencial:

- Robo de credenciales bancarias y datos financieros: Despliegue automatizado de ventanas superpuestas (overlays) maliciosas sobre aplicaciones bancarias legítimas para capturar nombres de usuario, contraseñas y datos de tarjetas.
- Control remoto total e inadvertido del dispositivo: Acceso interactivo que permite a los operadores manipular la interfaz del teléfono, realizar capturas de pantalla y controlar la unidad en tiempo real mientras la víctima observa una pantalla en negro o de actualización del sistema.
- Exfiltración de códigos de autenticación OTP e interacciones: La captura del árbol de la interfaz gráfica (UI Tree) y del teclado permite extraer mensajes SMS, tokens de verificación de doble factor e interacciones dentro de aplicaciones de mensajería o correo corporativo.
- Evasión y desactivación temporal de defensas móviles: La manipulación del tráfico mediante la VPN maliciosa aísla el comportamiento del malware impidiendo la detección y respuesta en la nube por parte de agentes de seguridad móviles.

Recomendaciones de mitigación:

1. Prohibición y restricción de la instalación desde fuentes desconocidas: Configurar políticas de gestión de dispositivos móviles (MDM) para bloquear la capacidad de instalar archivos APK fuera de la tienda oficial Google Play Store.
2. Auditoría estricta de permisos críticos de Android: Monitorear y restringir el otorgamiento de permisos de Servicios de Accesibilidad (Accessibility Services), permisos para establecer conexiones VPN no corporativas y la asignación de aplicaciones de inicio predeterminadas.
3. Implementación de defensas EDR/XDR en dispositivos móviles: Desplegar soluciones de protección en endpoints móviles para monitorear comportamientos anómalos, tales como solicitudes coordinadas de permisos de instalación junto con la creación de túneles VPN aislados.
4. Bloqueo perimetral de Indicadores de Compromiso (IoCs): Incorporar en las listas de bloqueo de firewall, DNS y soluciones Secure Web Gateway (SWG) las direcciones IP de infraestructura C2 reportadas (45.147.28.59 y 193.32.2.245) y los nombres de paquete maliciosos (io.base.one887, io.meat.hint).

Prioridad: Urgente.

Ampliar información:

- <https://www.punto-informatico.it/streamrat-malware-android-false-app-streaming/>
- <https://www.ingenieriatelematica.com.co/nuevo-troyano-streamrat-android-distribuye-malware-bancario-via-meta-ads/>
- <https://www.malwarebytes.com/blog/news/2026/09/streamrat-android-malware-spreads-through-meta-and-tiktok-ads>
- https://securityonline.info/streamrat-banking-trojan/#google_vignette
- <https://cyberpress.org/streamrat-seizes-android-devices/>

Recomendaciones generales sobre malware:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

PAPERCUT NG/MF – EXPLOTACIÓN ACTIVA DE VULNERABILIDADES ZERO-DAY PERMITE EJECUCIÓN REMOTA DE CÓDIGO SIN AUTENTICACIÓN (CVE-2026-81578 / CVE-2026-82078)

PaperCut Software ha emitido una alerta de seguridad urgente tras confirmar la explotación activa de dos vulnerabilidades críticas zero-day en sus soluciones de gestión de impresión PaperCut NG y PaperCut MF. La cadena de ataque encadenada permite a actores maliciosos remotos no autenticados modificar la configuración del sistema e inyectar código Java arbitrario, logrando la ejecución remota de código (RCE) en el servidor de aplicaciones. La exposición de estos servidores a internet representa un riesgo crítico de intrusión corporativa y despliegue de ransomware, por lo que se insta a aplicar los parches de emergencia de inmediato o aislar los entornos expuestos.

Resumen técnico:

- Identificador principal: CVE-2026-81578 y CVE-2026-82078.
- Severidad: Crítica (CVSS v4.0: 9.4 para CVE-2026-82078; CVSS v4.0: 8.8 para CVE-2026-81578 / Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).
- Causa raíz: Control de acceso inadecuado / elusión de autenticación en la interfaz web de gestión (CWE-306) y carga dinámica no segura de clases Java / reflexión insegura en utilidades de base de datos (CWE-470).
- Mecanismo de falla: Un atacante no autenticado envía solicitudes web especialmente diseñadas a la interfaz de administración, donde las comprobaciones de autorización fallan al validar las acciones del componente subyacente (CVE-2026-81578). Esto permite modificar parámetros de configuración de la base de datos para forzar la carga de clases Java no autorizadas (Udydn.class) desde el classpath, logrando la ejecución de bytecode Java arbitrario bajo el contexto del proceso del servidor pc-app.exe (CVE-2026-82078).
- Estado de explotación: Explotación activa en el entorno real confirmada desde el 27 de agosto de 2026 e incluida en el catálogo KEV de CISA. Se registran incidentes en organizaciones educativas y corporativas con ejecución de comandos de reconocimiento y despliegue de herramientas de acceso remoto.
- Versiones afectadas: PaperCut NG y PaperCut MF en sus versiones principales v24, v25 y v26 (así como versiones v23 y anteriores fuera de soporte).

Impacto potencial:

- Ejecución remota de código (RCE) y control total del servidor: Permite a atacantes anónimos ejecutar comandos arbitrarios del sistema operativo con privilegios elevados del proceso pc-app.exe, tomando control completo del servidor de aplicaciones de impresión.
- Punto de entrada para campañas de ransomware y extorsión: La vulnerabilidad es aprovechada por grupos cibercriminales para obtener acceso inicial a redes corporativas, desplegar malware secundario e iniciar cifrado o exfiltración de datos.
- Despliegue de herramientas de persistencia y movimiento lateral: Se ha observado la ejecución de comandos de reconocimiento de Active Directory (nltest), descarga de agentes de acceso remoto no autorizados (como SimpleHelp o AnyDesk) e instalación de servicios maliciosos en el sistema anfitrión.
- Exfiltración de documentos e información confidencial: El compromiso del servidor PaperCut otorga acceso a registros de impresión, datos de tarjetas de identificación, credenciales de usuarios y documentos confidenciales procesados en la cola de impresión de la organización.

Recomendaciones para mitigar el riesgo:

1. Aplicación prioritaria del parche de emergencia (Release 3): Desplegar de forma urgente la actualización de emergencia Release 3 en las versiones correspondientes (compilaciones 76530 a 76535 para ramas v24, v25 y v26) para corregir la cadena de explotación y regresiones conocidas.
2. Restringir inmediatamente el acceso público a internet al puerto web del servidor de aplicaciones PaperCut NG/MF mediante reglas de firewall o ACLs, permitiendo únicamente conexiones desde IP internas o redes de confianza.
3. Búsqueda activa de Indicadores de Compromiso (IoCs): Auditar los archivos de registro server.log en busca de cadenas anómalas (como jdbc:derby:memory:pwn o errores DatabaseUtils), revisar la presencia de archivos .class, .cmd o .out sospechosos en las carpetas server/lib y server/data/content, y verificar la eliminación atípica de registros.
4. Inspección de procesos hijo y servicios no autorizados: Monitorear el proceso pc-app.exe para detectar la creación de procesos hijo de consola (cmd.exe, powershell.exe) y auditar la presencia del servicio "Remote Access Service" (SimpleHelp) o ejecutables no autorizados en C:\ProgramData\.

Prioridad: Urgente.

Ampliar Información:

- <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>
- <https://devel.group/blog/explotacion-activa-en-papercut-ng-mf-permite-ejecucion-de-codigo-sin-autenticacion/>
- <https://www.huntress.com/blog/papercut-actively-exploited>
- <https://www.ingenieriatelematica.com.co/vulnerabilidad-zero-day-en-papercut-ng-y-mf-explotada-activamente-que-hacer/>
- <https://www.escudodigital.com/ciberseguridad/brecha-seguridad-software-gestion-impresoras-papercut.html>