

GammaCS-CERT
By Gamma Ingenieros



Boletín de Ciberseguridad Semanal

Edición °3726



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

CISCO SECURE FIREWALL MANAGEMENT CENTER (FMC) Y PRODUCTOS SEGURIDAD CISCO – MÚLTIPLES VULNERABILIDADES CRÍTICAS Y ZERO-DAY PERMITEN OBTENCIÓN DE ACCESO ROOT, EVASIÓN DE AUTENTICACIÓN Y EXPLOTACIÓN ACTIVA (CVE-2026-20079 / CVE-2026-20341 / CVE-2026-20340 / CVE-2026-20344)

Cisco ha publicado avisos de seguridad críticos e informes de amenazas tras confirmar la explotación activa en el entorno real de vulnerabilidades que afectan a Cisco Secure Firewall Management Center (FMC), Cisco Identity Services Engine (ISE) y software asociado (ASA/FTD). Las fallas principales permiten a atacantes remotos no autenticados o con permisos reducidos evadir los controles de autenticación, ejecutar comandos arbitrarios con privilegios de superusuario (root), realizar inyecciones SQL y descargar archivos confidenciales del sistema. Investigaciones de seguridad han documentado la explotación activa de estos fallos por parte de múltiples grupos de amenazas, incluyendo actores estatales y afiliados de ransomware.

Resumen técnico:

- Identificador principal: CVE-2026-20079, CVE-2026-20341, CVE-2026-20340, CVE-2026-20344 (junto a CVE-2026-20342 y CVE-2026-20343).
- Severidad: Crítica (CVSS v3.1: 10.0 para CVE-2026-20079; CVSS v3.1: 9.1 para CVE-2026-20341; CVSS v3.1: 8.8 para CVE-2026-20340 y CVE-2026-20344).
- Causa raíz: Creación de procesos de sistema impropios en el arranque (CWE-306), deserialización no segura de datos no confiables en el protocolo sftunnel (CWE-502), deserialización no segura en la gestión web y sanitización insuficiente de entradas de usuario en solicitudes HTTP (CWE-89 / CWE-22).
- Mecanismo de falla:
- CVE-2026-20079: Un proceso del sistema creado incorrectamente durante el arranque permite a un atacante no autenticado enviar peticiones HTTP manipuladas para ejecutar scripts en el dispositivo y obtener acceso directo con privilegios de root.
- CVE-2026-20341: La deserialización no segura en la comunicación entre dispositivos mediante el protocolo sftunnel permite a un usuario autenticado con credenciales administrativas en un equipo FTD gestionado enviar llamadas RPC manipuladas para ejecutar comandos con privilegios de root en el FMC.
- CVE-2026-20340: La deserialización de datos controlados por el usuario en la interfaz web permite a usuarios con roles de lectura (como Security Analyst) enviar cargas HTTP maliciosas y ejecutar comandos en el sistema operativo subyacente como root.
- CVE-2026-20344: La falta de validación en la interfaz de gestión web permite a usuarios con roles administrativos específicos ejecutar consultas SQL arbitrarias para extraer credenciales de sesión de administradores y datos de la base de datos.
- Estado de explotación: Confirmada la explotación activa en el entorno real de CVE-2026-20079 y fallos asociados por Cisco Talos. Se registra despliegue de web shells, troyanos como Cyclops Blink y actividades previas al despliegue de ransomware (Qilin).
- Versiones afectadas: Cisco Secure FMC en versiones de las ramas 7.0 (anteriores a 7.0.10), 7.2 (anteriores a 7.2.12), 7.4 (anteriores a 7.4.8), 7.6 (anteriores a 7.6.6), 7.7 (anteriores a 7.7.13), 10.0 (anteriores a 10.0.2) y 10.1 (anteriores a 10.1.0).

Impacto potencial:

- Toma de control total del dispositivo con privilegios de root: Permite a atacantes ejecutar comandos arbitrarios del sistema operativo con el máximo nivel de privilegios, facilitando el control absoluto sobre la infraestructura de gestión de firewalls.
- Despliegue de implantes persistentes y malware: Se ha documentado la instalación de web shells en directorios Tomcat, ejecutables JAR maliciosos y versiones del malware Cyclops Blink para mantener acceso persistente y control remoto.
- Compromiso y exfiltración de credenciales y datos de red: La explotación de inyecciones SQL y scripts de reconocimiento permite extraer hash de contraseñas de cuentas de Active Directory, MySQL, sesiones de administración e inventarios de red.
- Movimiento lateral y despliegue de ransomware corporativo: Sirve como punto de apoyo perimetral para establecer túneles SOCKS/SSH reversos hacia la red interna, permitiendo el despliegue posterior de ransomware en endpoints de la organización.

Recomendaciones de mitigación:

1. Aplicación prioritaria de parches e instaladores de seguridad (Hotfixes): Desplegar de inmediato las actualizaciones oficiales y versiones de mantenimiento recomendadas por el fabricante para las ramas afectadas de Cisco Secure FMC, ASA y FTD.
2. Restricción perimetral de interfaces de gestión: Bloquear la exposición hacia internet de las interfaces web de administración y puertos de control, limitando el acceso exclusivamente a rangos IP administrativos y redes segmentadas de confianza.
3. Auditoría e inspección activa de indicadores de compromiso (IoCs): Revisar los logs de la aplicación, el directorio webroot de CSM Tomcat y los procesos del sistema para detectar archivos inusuales (.jsp o .jar desconocidos), tareas modificadas o llamadas atípicas mediante el script package_info.pl.
4. Segmentación de red y rotación de credenciales: Aislar los dispositivos de gestión en zonas seguras, revocar y rotar inmediatamente credenciales de cuentas locales, claves de integración API y secretos de base de datos en caso de sospechar compromiso.

Prioridad: Crítica.

Ampliar información:

- <https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html>
- <https://www.bitsight.com/blog/critical-vulnerability-alert-cve-2026-76460-cisco-ise-authentication-bypass>
- <https://aviatrix.ai/threat-research-center/cisco-ise-zero-day-cve-2026-76460/>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-multivulns-4PsnFwvx>
- <https://blog.talosintelligence.com/fmc-ongoing-exploitation/>

PARALLELSS DESKTOP PARA MAC – VULNERABILIDAD DE INYECCIÓN DE ARGUMENTOS PERMITE ESCALADA LOCAL DE PRIVILEGIOS A ROOT ("PARASHELLS") (CVE-2026-90894)

Investigadores de seguridad de la firma JFrog han revelado una vulnerabilidad crítica de escalada de privilegios local (denominada "ParaShells") en el software de virtualización Parallels Desktop para Mac. El fallo (CVE-2026-90894) permite a un usuario local sin privilegios administrativos o a un proceso no autorizado ejecutar código arbitrario con privilegios de superusuario (root) en el sistema anfitrión macOS. La vulnerabilidad radica en la gestión insegura del servicio en segundo plano prl_disp_service, el cual expone un socket de dominio Unix con permisos de escritura globales y realiza una concatenación no sanitizada de parámetros al desempaquetar imágenes de máquinas virtuales.

Resumen técnico:

- Identificador principal: CVE-2026-90894 (denominado informalmente ParaShells).
- Severidad: Alta / Crítica (CVSS v3.1 / v4.0: 7.8 / Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Permisos de socket no restrictivos (CWE-276), autenticación de cliente local insuficiente y concatenación de comandos no sanitizada durante la extracción de paquetes/appliances (Inyección de argumentos / CWE-88).
- Mecanismo de falla:
- El servicio prl_disp_service se ejecuta con privilegios de root y escucha en el socket /var/run/prl_disp_service.socket, el cual cuenta con permisos de lectura y escritura globales (0777).
- La función de autenticación local PrlSrv_LoginLocal valida la conexión basándose en las credenciales enviadas por el kernel sin requerir firma de código de Parallels, permitiendo a usuarios estándar autenticarse.
- Durante la ejecución de PrlSrv_InstallAppliance, la aplicación construye una línea de comandos para la herramienta tar de macOS (tar -xf "%1" -C "%2"). Al inyectar una comilla doble dentro de la ruta elegida por el atacante, la función QProcess::splitCommand de Qt cierra prematuramente el parámetro e inyecta la opción --use-compress-program.
- Dado que tar es invocado con privilegios de root, la utilidad ejecuta el programa o script arbitrario especificado por el atacante bajo el contexto del superusuario.
- Estado de explotación: Divulgada públicamente a mediados de septiembre de 2026 por JFrog con la inclusión de pruebas de concepto (PoC). No se registra evidencia de explotación activa previa en el entorno real al momento de la publicación.
- Versiones afectadas: Parallels Desktop para Mac en todas las versiones anteriores a la rama 27 (confirmado en versiones 26.4.0 build 57513 y compilaciones 26.x)..

Impacto potencial:

- Escalada de privilegios locales a superusuario (root): Permite a cualquier usuario con acceso local o a código en ejecución sin privilegios tomar control total sobre el sistema operativo anfitrión Mac.
- Instalación de persistencia y evasión de defensas: Un atacante con privilegios de root puede registrar demonios de inicio no autorizados (launchd), alterar reglas de sudo y modificar componentes críticos del sistema operativo sin restricciones.
- Exfiltración y manipulación de información sensible: Otorga capacidades para leer, alterar o eliminar archivos, datos personales, claves de cifrado y documentos pertenecientes a otros usuarios en el equipo anfitrión.
- Compromiso mediante vectores de código no confiable: Facilita que herramientas de desarrollo comprometidas (como scripts de npm, fórmulas de Homebrew maliciosas o tareas de integración continua) escalen privilegios automáticamente al ser ejecutadas.

Recomendaciones de mitigación:

1. Actualización prioritaria a la versión 27 o posterior: Desplegar inmediatamente la actualización a Parallels Desktop versión 27.0.0 (o compilaciones 27.0.1 / superior), las cuales incluyen la corrección en la lógica de extracción de paquetes.
2. Restricción y auditoría de cuentas locales: Limitar el acceso interactivo y los privilegios de inicio de sesión local en equipos Mac que ejecuten el software afectado mientras se completa el proceso de actualización.
3. Inspección de permisos de sockets y procesos activos: Verificar la configuración del archivo `/var/run/prl_disp_service.socket` e inspeccionar ejecuciones inusuales del proceso `tar` o utilidades del sistema originadas por `prl_disp_service`.
4. Monitoreo de persistencia en macOS: Monitorear directorios de persistencia del sistema (tales como `/Library/LaunchDaemons` y `/Library/LaunchAgents`) para identificar la creación no autorizada de servicios o scripts de arranque.

Prioridad: Crítica.

Ampliar información:

- <https://thehackernews.com/2026/09/parallels-desktop-flaw-lets-non-admin.html>
- <https://www.helpnetsecurity.com/2026/09/16/parallels-desktop-cve-2026-90894-parashells-vulnerability/>
- <https://www.scworld.com/brief/parallels-desktop-flaw-allows-local-users-to-gain-root-access>
- <https://blog.elhacker.net/2026/09/vulnerabilidad-de-parallels-desktop.html>
- <https://www.geekmagazine.com/nueva-vulnerabilidad-critica-en-parallels-desktop-un-usuario-sin-privilegios-puede-tomar-el-control-total-de-tu-mac/>

LITESPEED WEB SERVER ENTERPRISE – VULNERABILIDAD CRÍTICA DE ESCALADA DE PRIVILEGIOS PERMITE EVADIR EL AISLAMIENTO DE INQUILINOS Y OBTENER ACCESO ROOT EN SERVIDORES COMPARTIDOS

cPanel ha emitido una alerta de seguridad urgente tras confirmarse una vulnerabilidad crítica de escalada de privilegios en el servidor web LiteSpeed Web Server Enterprise. El fallo permite a un usuario malicioso o a una cuenta de alojamiento web con privilegios reducidos romper las barreras de aislamiento multi-inquilino (incluyendo el entorno de restricción CloudLinux CageFS) y obtener acceso con privilegios de superusuario (root) al servidor anfitrión. La explotación exitosa compromete la totalidad de la infraestructura de alojamiento compartido, permitiendo el acceso, la modificación o el borrado no autorizado de datos de otros clientes alojados en la misma máquina.

Resumen técnico:

- Identificador principal: Aviso de Seguridad LiteSpeed Enterprise / cPanel (Pendiente de asignación oficial de CVE).
- Severidad: Crítica (Clasificado como Crítico por cPanel / Prioridad de parcheo inmediato por romper límites de aislamiento multi-inquilino).
- Causa raíz: Fallo de control de acceso e inspección de límites de autorización en el proceso principal del servidor web (Evasión de aislamiento de inquilinos / CWE-269).
- Mecanismo de falla:
- Un usuario autenticado en una cuenta básica de hosting (o un proceso dentro de un sitio web comprometido) ejecuta una solicitud o script diseñado contra el proceso de LiteSpeed Web Server.
- La vulnerabilidad permite al proceso del usuario evadir los controles del sistema de archivos restringido impuestas por herramientas de aislamiento como CloudLinux CageFS.
- Al romper el entorno restringido, la solicitud se procesa fuera del sandbox del cliente, permitiendo la ejecución de comandos con los privilegios elevados (root) con los que opera el servicio del servidor web.
- Estado de explotación: Divulgada oficialmente el 14 de septiembre de 2026 por cPanel. Se insta a realizar el parcheo manual inmediato, ya que la propagación a través de los canales de actualización automática del fabricante puede presentar retrasos.
- Versiones afectadas: LiteSpeed Web Server Enterprise en todas las versiones anteriores a la 6.3.7 (específicamente versiones anteriores a la v6.3.7 Build 2).

Impacto potencial:

- Escalada de privilegios a nivel de superusuario (root): Permite a cualquier usuario de una cuenta de hosting estándar tomar control administrativo absoluto sobre el sistema operativo del servidor.
- Compromiso total de entornos de alojamiento compartido (Shared Hosting): Al evadir la protección de CageFS, un atacante puede acceder a los archivos, bases de datos, aplicaciones y entornos de todos los demás clientes alojados en el mismo servidor.
- Exfiltración de credenciales y datos confidenciales: Otorga capacidad para leer archivos de configuración globales, claves de cifrado, secretos de bases de datos y credenciales de acceso almacenadas en el servidor.
- Despliegue de código malicioso y persistencia en la infraestructura: Un atacante con privilegios de root puede instalar puertas traseras, alterar servicios del sistema o utilizar el servidor como nodo para actividades maliciosas.

Recomendaciones de mitigación:

1. Actualización manual e inmediata a la versión v6.3.7 Build 2: Ejecutar de forma prioritaria el comando oficial de actualización forzada `/usr/local/lsws/admin/misc/lswsup.sh -f -v 6.3.7` seguido del reinicio del servicio (`/usr/local/lsws/bin/lswsctrl restart`).
2. Auditoría e inspección de integridad de servidores compartidos: Inspeccionar el sistema en busca de procesos atípicos ejecutándose como root, archivos modificados recientemente fuera de los directorios `/home/` y tareas programadas (cron) no autorizadas.
3. Revisión de cuentas de hosting y permisos de ejecución: Verificar el estado de los usuarios locales en el servidor y monitorear cuentas de hosting que tengan habilitado el acceso por shell (SSH) o comandos de ejecución remota.
4. Verificación de logs y actividad anómala: Auditar los registros web de LiteSpeed y cPanel para identificar intentos atípicos de acceso a archivos del sistema o comportamiento anómalo originado desde cuentas de usuario individuales.

Prioridad: Crítica.

Ampliar información:

- <https://vserve.com/litespeed-enterprise-vulnerability-root-access-6-3-7/>
- <https://support.cpanel.net/hc/en-us/articles/43483286674583-Security-LiteSpeed-Enterprise-security-advisory-September-14-2026>
- <https://securityaffairs.com/199127/security/shared-hosting-at-risk-litespeed-enterprise-bug-can-grant-root-from-a-single-tenant.html>
- <https://thehackernews.com/2026/09/litespeed-enterprise-flaw-could-let-one.html>
- <https://mallory.ai/stories/01a0a454-6fe9-71b8-8ff0-b306a07ed895>

MALWARE

MALWARE — KREMLIN: ECOSISTEMA DE MALWARE BANCARIO EXTERNO EXPLOTA LOS CHECKPOINTS DE INTEGRIDAD DE CHROMIUM PARA INSTALAR EXTENSIONES MALICIOSAS Y ROBAR SESIONES EN CHROME Y EDGE

Investigadores de ciberseguridad de Elastic Security Labs y reportes del sector de ciberseguridad (incluyendo alertas del CSIRT Financiero) han identificado las operaciones del malware denominado KREMLIN. Este sofisticado ecosistema malicioso y troyano bancario para entornos Windows infecta dispositivos a través de cargadores JavaScript y scripts maliciosos de varias etapas. Una vez en el sistema, KREMLIN manipula los archivos de preferencias e integridad del navegador (Secure Preferences), burlando las verificaciones criptográficas de Chromium para instalar de forma silenciosa extensiones maliciosas (como AVSync) en Google Chrome y Microsoft Edge. Su objetivo principal es la captura de tokens de sesión, cookies, credenciales bancarias y el monitoreo en tiempo real del tráfico web de las víctimas.

Resumen técnico:

- Identificador principal: Ecosistema de Malware Bancario e Infostealer KREMLIN / Extensión Maliciosa AVSync (asociado a la campaña REF9334).
- Tipo de amenaza: Troyano bancario (Banking Trojan), Extractor de información (Infostealer) y Extensión maliciosa de navegador (Malicious Browser Extension).
- Mecanismo de acceso e infección: La cadena de ataque inicia mediante ingeniería social (phishing), distribuyendo archivos JavaScript (.js) disfrazados de facturas, recibos bancarios o documentos comerciales. Tras superar las comprobaciones anti-sandbox, descarga utilidades en segundo plano (como entornos Node.js), crea tareas programadas para garantizar la persistencia y consulta contratos inteligentes en la cadena de bloques de Ethereum para resolver de forma dinámica las direcciones IP de su infraestructura de Comando y Control (C2) mediante mecanismos de dead-drop resolver.
- Capacidades avanzadas y manipulación de navegador:
- Manipulación de preferencias de Chromium: El malware aguarda a que el usuario cierre el navegador (o fuerza su cierre por inactividad), copia la extensión al directorio de perfil y la registra en el archivo Secure Preferences activando el modo desarrollador. Para evitar que Chromium la deshabilite por corrupción, recupera las claves de cifrado del navegador y re-calcula los valores HMAC y hashes de integridad.
- Acciones de la extensión (AVSync): Inyecta código HTML malicioso en sitios bancarios, monitorea el teclado (keylogging) en formularios, realiza capturas de pantalla, intercepta peticiones HTTP/WebSocket, extrae almacenamiento local (LocalStorage y sessionStorage), cookies de autenticación y redirecciona clics hacia portales fraudulentos.
- Evasión y carga de artefactos: Utiliza técnicas de carga lateral de bibliotecas DLL (DLL Side-Loading) mediante binarios legítimos (como ejecutables de SentinelOne) y aloja componentes secundarios ocultos en archivos JPEG dentro de repositorios públicos como Internet Archive.
- Estado de actividad: Campaña activa reportada con mayor impacto en entidades bancarias y usuarios finales en América Latina (con foco principal en Brasil) y expansión progresiva a otras regiones.

Impacto potencial :

- Secuestro de sesiones y robo de credenciales bancarias: La captura de tokens de sesión activos y cookies permite a los atacantes suplantar la identidad de la víctima en plataformas bancarias y portales corporativos sin requerir credenciales de primer factor.
- Manipulación en tiempo real del contenido web: La capacidad de inyectar código HTML en tiempo real permite alterar los formularios de transferencias o superponer pantallas falsas para engañar al usuario durante transacciones financieras.
- Exfiltración de claves y datos sensibles del navegador: Extrae bases de datos internas del navegador, historial de navegación, certificados y las claves criptográficas App-Bound Encryption requeridas para descifrar contraseñas guardadas en el sistema.
- Persistencia en el sistema anfitrión: La creación de tareas programadas en Windows y el uso de herramientas de acceso remoto (como REMCOS RAT) otorgan acceso continuo y no autorizado al equipo comprometido.

Recomendaciones de mitigación:

1. Monitoreo e inspección de archivos de configuración de Chromium: Configurar reglas de auditoría en soluciones EDR para detectar modificaciones no autorizadas en el archivo Secure Preferences y en las rutas de perfil de Chrome y Edge (AppData\Local\Google\Chrome\User Data\...).
2. Supervisión de ejecuciones no autorizadas y tareas programadas: Monitorear y restringir la creación de tareas programadas que invoquen binarios inusuales de Node.js, ejecuciones sospechosas de PowerShell o comportamiento anómalo asociado a herramientas legítimas de seguridad utilizadas para carga lateral.
3. Auditoría de extensiones de navegador a nivel corporativo: Aplicar directivas de grupo (GPO) o políticas de gestión centralizada para forzar listas blancas de extensiones permitidas (ExtensionInstallAllowlist) y bloquear la instalación de extensiones en modo desarrollador o desde fuentes no oficiales.
4. Bloqueo de red y restablecimiento de sesiones: Monitorear y denegar conexiones hacia nodos o contratos de Ethereum no autorizados, bloquear dominios e IPs C2 conocidos y proceder al cierre de sesiones activas e hipervinculadas y rotación de contraseñas de usuarios que presenten alertas.

Prioridad: Urgente.

Ampliar información:

- <https://tech.yahoo.com/cybersecurity/articles/chrome-edge-browsers-hijacked-kremlin-100500988.html>
- <https://www.softzone.es/noticias/seguridad/malware-kremlin-extensiones-chrome-edge/>
- <https://hipertextual.com/seguridad/nuevo-malware-kremlin-instala-extensiones-de-chrome-y-roba-tus-datos/>
- <https://csirtasobancaria.com/alertas-de-seguridad/kremlin-malware-bancario-explota-chrome-y-edge-para-secuestrar-sesiones-de-los-usuarios>
- <https://socprime.com/es/active-threats/la-extension-que-nunca-instalo-el-kremlin-falsifica-los-cheques-de-integridad-de-chrome-para-robar-sesiones-bancarias/>

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

REVOLUT – ATAQUE DE SUPLANTACIÓN DE IDENTIDAD GUBERNAMENTAL (SPOOFING) Y SOLICITUDES FRAUDULENTAS EXPONEN DATOS SENSIBLES DE CLIENTES Y DERIVAN EN EXTORSIÓN CON RANSOMWARE

El neobanco y plataforma de tecnología financiera Revolut confirmó haber sido víctima de una brecha de seguridad originada por una sofisticada campaña de suplantación de identidad (spoofing). Actores maliciosos utilizaron el dominio de correo electrónico legítimo de una agencia gubernamental (presumiblemente de origen italiano) para enviar solicitudes fraudulentas de información. Al considerar legítima la procedencia del correo, personal de la entidad respondió entregando información confidencial, escaneos de documentos de identidad y registros transaccionales de clientes. Días después de la filtración, los atacantes iniciaron un intento de extorsión exigiendo un rescate millonario bajo amenaza de publicar los datos.

Resumen técnico:

- Identificador principal: Brecha de Seguridad y Filtración de Datos de Revolut / Ataque de Suplantación de Dominio Gubernamental (Grooming / Spoofing) / Campaña de Extorsión de iamnotavillain.
- Severidad: Importante / Alta (Incidentes de Privacidad, Exfiltración de Datos Personales y Extorsión a Entidad Financiera).
- Causa raíz: Suplantación de identidad y spoofing de correo electrónico desde un dominio de nivel gubernamental legítimo comprometido (Ingeniería social orientada a empleados / Verificación insuficiente de solicitudes de información regulatoria).
- Mecanismo de falla:
- Un tercero no autorizado obtuvo acceso o capacidades de envío desde la infraestructura de correo de una autoridad pública (agencia gubernamental).
- Los atacantes enviaron una solicitud formal de información de clientes simulando un requerimiento legal o judicial legítimo.
- Al provenir de una dirección con un dominio oficial y legítimo, los mecanismos de filtro y la verificación humana validaron la petición, derivando en la entrega no autorizada de paquetes de datos confidenciales de usuarios seleccionados.
- Tras obtener los datos, el grupo cibercriminal (auto-identificado como iamnotavillain) publicó una demanda de rescate de 3 millones de dólares en la criptomoneda Monero (XMR) para evitar la filtración pública de la información.
- Estado de actividad: Incidente detectado y notificado a mediados de septiembre de 2026. La entidad bloqueó el dominio de origen, notificó a las agencias de protección de datos (como la ICO en el Reino Unido), a los reguladores financieros y contactó de forma directa a los usuarios afectados.
- Impacto y alcance: Aunque la compañía definió el alcance como "muy limitado", reportes internacionales indican un aproximado de 680 clientes afectados a nivel global (25 de ellos en España). Se confirmó que los fondos y los sistemas bancarios centrales de Revolut no sufrieron un compromiso directo.

Impacto potencial:

- Exfiltración de documentos de identidad y datos de verificación: Compromiso de imágenes escaneadas de pasaportes, DNI/licencias de conducción y fotografías faciales de validación (selfies de autenticación).
- Exposición de información bancaria y financiera: Filtración de números de cuenta (IBAN), historial de transacciones, extractos bancarios y registros de compra/venta de criptomonedas.
- Aumento en el riesgo de fraude y suplantación de identidad secundaria: Los datos expuestos facultan a los atacantes para realizar ataques dirigidos de phishing, SIM swapping o suplantación de identidad contra los usuarios afectados utilizando información verídica para engañarlos.
- Riesgo de extorsión y daño reputacional: Exposición de clientes con carteras elevadas de activos y presión de extorsión económica pública sobre la institución financiera.

Recomendaciones para mitigar el riesgo:

1. Fortalecimiento de protocolos de validación de solicitudes gubernamentales: Establecer canales de verificación fuera de banda (Out-of-Band Verification) obligatorios para la entrega de datos de clientes solicitados por entes reguladores o agencias públicas (verificación telefónica previa, autenticación por portales oficiales o firmas digitales).
2. Implementación estricta de mecanismos de autenticación de correo: Reforzar políticas de validación SPF, DKIM y DMARC en pasarelas de correo y evaluar herramientas de seguridad que analicen la reputación y anomalías en el comportamiento o solicitudes atípicas de información sensible.
3. Apoyo y monitoreo de identidades afectadas: Ofrecer servicios de monitoreo de crédito, protección contra el fraude e identidades para los clientes cuyos documentos personales e IBAN fueron expuestos.
4. Capacitación continua en prevención de ingeniería social avanzada: Capacitar al personal operativo y legal en la identificación de solicitudes fraudulentas que se originen desde cuentas corporativas o gubernamentales previamente comprometidas.

Prioridad: Urgente.

Ampliar Información:

- <https://www.reuters.com/legal/litigation/revolut-confirms-sensitive-customer-data-breach-falling-fake-government-requests-2026-09-12/>
- <https://www.eleconomista.es/banca-finanzas/noticias/14014015/09/26/revolut-sufre-una-brecha-de-seguridad-en-los-datos-de-sus-clientes-con-700-afectados-a-nivel-global-y-25-en-espana.html>
- <https://www.xataka.com/seguridad/brecha-seguridad-revolut-no-fue-hackeo-fue-creerse-email-falso>
- <https://es.marketscreener.com/noticias/revolut-confirma-una-brecha-de-datos-confidenciales-tras-caer-en-peticiones-gubernamentales-falsas-ce785bdcd989f220>
- <https://es.investing.com/news/stock-market-news/filtracion-de-datos-de-revolut-afecta-a-casi-700-clientes-3834209>