GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2826

BOLETÍN DE CIBERSEGURIDAD SEMANAL

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 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

CVE-2026-15409 / CVE-2026-15410 – SONICWALL SMA 1000 ZERO-DAY (FALSIFICACIÓN DE SOLICITUDES DEL LADO DEL SERVIDOR Y EJECUCIÓN DE CÓDIGO REMOTO)

Se ha divulgado de forma urgente la explotación activa en entornos reales de dos vulnerabilidades de día cero (Zero-Day) que afectan de manera crítica a los dispositivos de acceso remoto seguro de la serie SonicWall Secure Mobile Access (SMA) 1000. El fallo principal permite a un actor de amenazas remoto no autenticado comprometer el perímetro de la red mediante una falsificación de solicitudes del lado del servidor (SSRF), abriendo una pasarela directa para encadenar la ejecución de comandos arbitrarios del sistema operativo con privilegios de root.

Los appliances, al operar de forma centralizada en la frontera perimetral proporcionando acceso SSL VPN a redes corporativas, multinacionales y organismos gubernamentales, representan un riesgo operativo crítico si son comprometidos. La cadena de explotación permite eludir los controles de acceso tradicionales, obtener control total del sistema operativo y establecer mecanismos de persistencia indetectables a largo plazo.

Resumen técnico:

- Identificador principal: CVE-2026-15409 y CVE-2026-15410.
- Severidad: Crítica / Alta (Puntaje base de 10.0 para CVE-2026-15409 y 7.2 para CVE-2026-15410 bajo el estándar CVSS v3.1).
- Causa raíz: CVE-2026-15409 radica en una vulnerabilidad de Server-Side Request Forgery (SSRF) en la interfaz pública Workplace, mientras que CVE-2026-15410 se debe a una inyección de código post-autenticación originada por un defecto lógico de recorrido de ruta (Path Traversal) en el flujo de trabajo de eliminación de parches de la Appliance Management Console (AMC).
- Mecanismo de falla: El ataque inicial abusa de la característica de proxy WebSocket a través de la ruta /wsproxy. Al manipular los parámetros de la URL, el atacante abre un túnel TCP hacia servicios restringidos que escuchan únicamente en el localhost del appliance (tales como el proceso Erlang en el puerto 1050 o el servicio ctrl-service en el puerto 8188), evadiendo la autenticación perimetral. Posteriormente, para consolidar el control, explota el CVE-2026-15410 enviando una solicitud POST maliciosa a /rollbackConfirm.action que apunta a un script malicioso alojado en directorios temporales (ej. ../../../../../tmp/payload.sh). El sistema otorga permisos de ejecución de manera automática y procesa el script con privilegios avanzados de Root (UID=0), forzando un reinicio inmediato del gateway.
- Estado de explotación: Explotación activa confirmada en la práctica (in the wild). La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) ha incorporado de inmediato ambos fallos a su catálogo de Vulnerabilidades Explotadas Conocidas (KEV). Los análisis forenses de Rapid7 y Volexity demuestran que múltiples actores de amenazas han encadenado con éxito ambas fallas de manera dirigida desde finales de junio de 2026.
- Versiones afectadas: Modelos de hardware y virtuales de la serie SonicWall SMA 1000 (específicamente los modelos SMA6210, SMA7210 y SMA8200v) que ejecuten las versiones de firmware basadas en las ramas 12.4.3 (versiones 12.4.3-03245, 12.4.3-03387 y 12.4.3-03434) y 12.5.0 (versiones 12.5.0-02283, 12.5.0-02624 y 12.5.0-02800). Se confirma que el fallo no afecta a la línea SMA 100 ni a las funciones SSL VPN nativas de los firewalls estándar de SonicWall.

Impacto potencial:

- Movimiento lateral directo al Directorio Activo sin túnel VPN: Una vez tomado el control del appliance, los atacantes se saltan la necesidad de establecer una sesión VPN legítima. Utilizan la propia dirección IP interna del dispositivo y la cuenta de servicio LDAP integrada para lanzar solicitudes de autenticación NTLM anómalas contra los controladores de dominio principales de la empresa. Al emplear nombres de cliente de estaciones de trabajo no inventariadas (como kali), subvierten el monitoreo de identidad y actúan como un backdoor directo hacia la infraestructura del directorio.
- Extracción masiva de credenciales y semillas MFA: Al poseer capacidades de lectura y ejecución de nivel root dentro del sistema operativo subyacente, los actores de amenazas extraen de forma sistemática bases de datos de sesiones web activas, credenciales de alta prioridad almacenadas en caché y configuraciones de semillas de contraseñas de un solo uso basadas en tiempo (MFA TOTP). Esta recolección local les garantiza persistencia e ingresos encubiertos de largo plazo, capaces de sobrevivir a remediaciones estándar de red.
- Pivotaje encubierto y mapeo de la Intranet corporativa: Al abusar del túnel WebSocket provisto por la vulnerabilidad SSRF inicial, el dispositivo perimetral se transforma en un nodo proxy encubierto operado por el atacante. Desde este punto de apoyo, el actor de amenazas puede sondear, escanear y direccionar tráfico malicioso TCP hacia aplicaciones, bases de datos y segmentos internos restringidos de la intranet corporativa que no se encuentran expuestos de manera directa a Internet.
- Pérdida total de integridad y confidencialidad del Gateway de seguridad: Al comprometerse los privilegios de administración del sistema, los atacantes adquieren la facultad de implantar Web Shells, modificar configuraciones de enrutamiento globales, manipular o eliminar bitácoras de auditoría internas para imposibilitar las tareas forenses del SOC, o sabotear la disponibilidad del servicio de conectividad empresarial provocando denegaciones de servicio y caídas cíclicas de la plataforma mediante comandos forzados de apagado.

Recomendaciones de mitigación:

1. Aplicación prioritaria e inmediata de la actualización oficial de firmware: Se urge de manera mandatoria a los administradores de infraestructura a descargar e instalar los parches de seguridad oficiales provistos por el fabricante en el portal MySonicWall. Las plataformas afectadas deben migrar inmediatamente a la versión 12.4.3-03453 (o superior) para la rama de firmware 12.4.3, o a la versión 12.5.0-02835 (o superior) en caso de implementar la rama 12.5.0. Se advierte que no existen mitigaciones alternativas ni workarounds válidos en el software.
2. Activación del protocolo de respuesta a incidentes y redespliegue de entornos: En caso de que se verifique la existencia de cualquier indicador de compromiso previo, el simple parcheo del firmware es insuficiente para garantizar la remediación. Las organizaciones deben proceder al restablecimiento completo de imágenes de fábrica (re-imaging) en appliances físicos de hardware o al redespliegue desde cero de las plantillas de dispositivos virtuales. Posteriormente, se debe ejecutar un cambio masivo de contraseñas de usuarios y administradores, junto con el reseteo obligatorio de los tokens de autenticación TOTP.
3. Auditoría y cacería de amenazas heurística en bitácoras locales del dispositivo: Implementar revisiones exhaustivas y búsquedas manuales sobre los registros del sistema operativo para identificar firmas de explotación: inspeccionar el archivo extraweb_access.log en busca de peticiones con código de estado HTTP 200 dirigidas a / __api__/login o / __api__/logout (URIs inexistentes en configuraciones legítimas) y solicitudes HTTP 101 hacia /wsproxy que carguen parámetros de host sospechosos vinculados a localhost o 127.0.0.1. Asimismo, auditar ctrl-service.log rastreando invocaciones de remove_hotfix con caracteres de recorrido de directorios (../).
4. Aislamiento del plano de gestión y monitoreo de Directorio Activo: Restringir el acceso a la consola AMC mediante ACLs y firewalls, evitando su exposición a Internet y permitiendo únicamente el acceso desde segmentos de administración aislados o bastiones seguros. Complementariamente, configurar alertas en el SIEM para detectar inicios de sesión de Windows (Event ID 4624, Logon Tipo 3) originados desde la IP interna del appliance SonicWall SMA, especialmente cuando involucren estaciones no corporativas.

Prioridad: Crítica.

Ampliar información:

- https://unaaldia.hispasec.com/sonicwall-publica-hotfixes-tras-detectar-ataques-reales-contra-dos-zero-days-en-sma1000/
- https://devel.group/blog/explotacion-activa-zero-day-en-dispositivos-sonicwall-sma1000-cvss-10-0/
- https://www.rapid7.com/blog/post/etr-rapid7-mdr-team-discovers-new-sonicwall-sma1000-zero-days-being-actively-exploited-cve-2026-15409-cve-2026-15410/
- https://www.helpnetsecurity.com/2026/07/14/sonicwall-sma-attacks-via-cve-2026-15409-cve-2026-15410/
- https://thehackernews.com/2026/07/two-sonicwall-sma-1000-zero-days.html

CVE-2026-44747, CVE-2026-27690 Y CVE-2026-44761 – CLUSTER DE VULNERABILIDADES CRÍTICAS EN EL ECOSISTEMA SAP (CICLO DE PARCHES DE JULIO 2026)

Como parte de su ciclo global de actualizaciones de seguridad correspondiente a julio de 2026, SAP ha emitido un conjunto de advertencias críticas de máxima prioridad (HotNews) que abordan múltiples fallos graves en sus plataformas centrales. La principal vulnerabilidad (CVE-2026-44747) expone al motor de ejecución de aplicaciones empresariales SAP NetWeaver AS ABAP a corrupciones severas de memoria interna. En paralelo, se han divulgado fallas críticas adicionales que facilitan el secuestro de tráfico web en la pasarela SAP Approuter y la toma de control de servicios API mediante secretos predecibles en la plataforma transaccional SAP Commerce Cloud.

Debido a que el ecosistema SAP soporta funciones críticas como ERP, finanzas, cadena de suministro, nómina y operaciones comerciales, estas vulnerabilidades representan un riesgo de negocio crítico. Su explotación puede comprometer la confidencialidad de la información, permitir la alteración de registros transaccionales y provocar la interrupción total de los servicios productivos.

Resumen técnico:

- Identificadores principales: CVE-2026-44747 (Fallo primario en el Kernel), CVE-2026-27690 (Fallo de red en Approuter) y CVE-2026-44761 (Fallo de identidad en Commerce Cloud).
- Severidad: Crítica (Puntajes base de 9.9 para CVE-2026-44747, y de 9.1 para CVE-2026-27690 y CVE-2026-44761 bajo el estándar CVSS v3.1).
- Causa raíz: CVE-2026-44747 se clasifica como una vulnerabilidad de escritura fuera de límites (Out-of-Bounds Write / CWE-787) generada por errores lógicos en la gestión de buffers de memoria. Por su parte, CVE-2026-27690 es una falla de contrabando de peticiones HTTP (HTTP Request/Response Smuggling), mientras que CVE-2026-44761 consiste en el uso de credenciales cableadas por defecto (Default Credentials) heredadas de plantillas de documentación técnica.
- Mecanismo de falla: * En el fallo de NetWeaver ABAP, un usuario autenticado con privilegios mínimos puede explotar la debilidad lógica de gestión de memoria para corromper estructuras de datos adyacentes de la aplicación, logrando manipular código en ejecución.
- En SAP Approuter, un atacante remoto no autenticado puede enviar secuencias HTTP anómalas diseñadas de tal forma que el balanceador perimetral frontal y los sistemas back-end interpreten los límites de los mensajes de manera asíncrona (desincronización de petición/respuesta), exponiendo respuestas privadas de otros usuarios legítimos.
- En SAP Commerce Cloud, el riesgo se activa si el cliente importó scripts de configuración de ejemplo del Portal de Ayuda de SAP a producción sin modificar las llaves secretas; esto permite a un atacante no autenticado emplear credenciales públicamente documentadas para emitir tokens de acceso OAuth 2.0 válidos y consumir las APIs de la tienda virtual.

- Estado de explotación: No se dispone de evidencia pública sobre explotación activa en entornos reales (in the wild) al momento de su divulgación. Sin embargo, dada la criticidad intrínseca de los sistemas de planificación de recursos institucionales (ERP) y la publicación de los detalles técnicos, se anticipa una rápida integración en flujos automatizados de escaneo táctico.
- Versiones afectadas: * SAP NetWeaver AS ABAP: Versiones de Kernel KRNL64NUC (7.22, 7.22EXT) y KRNL64UC (7.22, 7.53, 7.54, 7.77, 7.89, 7.93, así como las ramas de la 9.16 a la 9.20).
- SAP Approuter: Versiones de paquetes basadas en Node.js anteriores a la 20.10.0 que operen de forma exclusiva fuera de entornos Cloud Foundry.
- SAP Commerce Cloud: Entornos de producción e instancias de comercio electrónico que conserven activo el cliente OAuth 2.0 de ejemplo provisto de fábrica.

Impacto potencial:

- Modificación no autorizada y manipulación de registros en el Core ERP: La explotación de la corrupción de memoria en NetWeaver ABAP fractura los límites de aislamiento de la base de datos de la aplicación. Un atacante con acceso básico de ejecución puede alterar de forma maliciosa datos maestros corporativos que residen dentro de implementaciones de SAP ERP o entornos avanzados SAP S/4HANA (tales como bases de datos financieras, registros de compras, flujos de proveedores o información confidencial de nóminas).
- Fuga masiva de datos y secuestro de sesiones mediante Request Smuggling: El desalineamiento en la interpretación de fronteras HTTP dentro de SAP Approuter permite la interceptación pasiva y activa de las comunicaciones de la plataforma de cara a internet. Los atacantes pueden secuestrar las respuestas destinadas a usuarios legítimos, facilitando la exfiltración de tokens de sesión activos, datos confidenciales de navegación de clientes y credenciales de autenticación expuestas en el flujo de tráfico web desincronizado.
- Infiltración total y control de APIs transaccionales en portales Commerce Cloud: El uso exitoso de credenciales OAuth 2.0 documentadas de acceso público otorga de forma inmediata un token de portador (Bearer Token) con privilegios para interactuar con las interfaces API de la plataforma de comercio digital. Esto permite a agentes externos vaciar catálogos de productos, exfiltrar bases de datos de pedidos de clientes, inyectar órdenes fraudulentas o alterar los métodos de pago establecidos en portales e-commerce corporativos.
- Denegación de servicio (DoS) e indisponibilidad de procesos de negocio neurálgicos: Las anomalías lógicas introducidas en la memoria del kernel ABAP y las desincronizaciones de tráfico masivo generadas en Approuter conducen a fallas catastróficas del sistema, provocando volcados de memoria (short dumps), caídas forzadas de las instancias de aplicación de producción y la congelación total de portales transaccionales interactivos (como SAP GUI para HTML), paralizando la continuidad operativa global de la organización.

Recomendaciones de mitigación:

1. Despliegue inmediato de actualizaciones de Kernel SAP y Notas de Seguridad: Priorizar e instalar de manera urgente la actualización oficial del Kernel ABAP especificada por el fabricante en la Nota de Seguridad Central 3747367 (y las ampliaciones del ciclo de parches de julio). De igual manera, es indispensable desplegar la actualización de paquetes correspondiente a la Nota 3727078 para proteger las implementaciones asociadas al contenedor web de NetWeaver, aislando las interfaces expuestas a internet mediante revisiones exhaustivas de control de cambios.
2. Auditoría física y purga de clientes OAuth con credenciales por defecto: Examinar de forma exhaustiva el repositorio de configuraciones de seguridad en las instancias de producción de SAP Commerce Cloud. Validar si el cliente OAuth 2.0 de ejemplo documentado en el portal de ayuda técnica se encuentra desplegado de manera residual; de confirmarse su presencia, se debe proceder a su remoción total o, en su defecto, a la sustitución obligatoria del secreto cableado por una cadena criptográfica de alta entropía y uso exclusivo.
3. **Actualización de SAP Approuter y endurecimiento de redirecciones:** Actualizar SAP Approuter a la versión 20.10.0 o superior para corregir las fallas en la delimitación de solicitudes HTTP. Además, configurar listas de control de acceso (Allowlists) que restrinjan estrictamente las URLs de redireccionamiento permitidas por la pasarela de autenticación, conforme a las directrices de la CVE-2026-44745.
4. **Evaluación de mitigaciones lógicas temporales (SICF):** Cuando la aplicación del parche del Kernel requiera una ventana prolongada de mantenimiento, evaluar la mitigación temporal de SAP mediante la deshabilitación selectiva de nodos del Internet Communication Framework (ICF) con la transacción SICF. Esta medida desactiva temporalmente el inicio de transacciones globales vía SAP GUI para HTML, por lo que su impacto debe validarse previamente en un entorno de pruebas (Staging).

Prioridad: Crítica.

Ampliar información:

- https://www.heise.de/en/news/Partially-critical-security-vulnerabilities-fixed-in-several-products-11364098.html
- https://vulert.com/blog/sap-netweaver-abap-cve-2026-44747/
- https://erp.today/sap-july-2026-patch-day-erp-security-coordination/
- https://fieldeffect.com/blog/sap-patches-critical-vulnerabilities
- https://www.mallory.ai/stories/019f5e60-31d1-7c4f-84d1-f77e82315fde
- https://thehackernews.com/2026/07/sap-patches-cvss-99-netweaver-abap-flaw.html

CVE-2026-57219 Y CVE-2026-57221 – RABBITMQ (FUGA DE SECRETOS OAUTH E INTERCEPTACIÓN DE METADATOS MULTI-INQUILINO)

Se han revelado dos fallos de seguridad relacionados con el control de acceso en el popular bróker de mensajería de código abierto RabbitMQ, el cual actúa de forma crítica como la infraestructura de tuberías (plumbing) que distribuye, enruta y procesa datos asíncronos (como órdenes de pago, autenticaciones y notificaciones internas) en aplicaciones modernas. La vulnerabilidad más severa (CVE-2026-57219) permite a un atacante remoto no autenticado extraer el secreto de cliente OAuth confidencial del servidor a través de una sola petición HTTP directa. El segundo fallo (CVE-2026-57221) rompe el aislamiento en implementaciones multi-inquilino corporativas, permitiendo la fuga pasiva de metadatos estructurales de las colas de procesamiento.

Debido a la amplia adopción de RabbitMQ en arquitecturas de microservicios y entornos basados en contenedores, estas vulnerabilidades representan un objetivo estratégico para los atacantes. Si el puerto de gestión está expuesto, pueden comprometer la capa de mensajería, obtener control de la infraestructura o acceder a información operativa sensible de los flujos de negocio.

Resumen técnico:

- Identificadores principales: CVE-2026-57219 y CVE-2026-57221.
- Severidad: Alta / Media (Puntaje base de 8.7 para CVE-2026-57219 y 5.3 para CVE-2026-57221 bajo el estándar CVSS v4.0).
- Causa raíz: CVE-2026-57219 se origina por la presencia residual de un punto de enlace HTTP obsoleto en la interfaz de administración web que carece de verificaciones operativas. CVE-2026-57221 se produce por una omisión en la validación de permisos lógicos (missing authorization check) durante la declaración pasiva de recursos del bróker.
- Mecanismo de falla: * El vector crítico (CVE-2026-57219) radica en el endpoint de gestión GET /api/auth. A diferencia del resto de componentes restringidos de la interfaz técnica, el control de autorización de esta ruta web fue programado de manera cableada (hard-coded) para validar y responder de forma afirmativa a cualquier solicitud entrante sin requerir credenciales. Al invocarlo en instancias que usen el parámetro management.oauth_client_secret, el servidor imprime en texto claro la llave secreta de cliente OAuth. Con esta clave, el atacante recurre al proveedor de identidad de la empresa (Keycloak, Azure AD/Entra ID, Auth0) para firmar un token con rol de administrador y secuestrar el clúster.
- En el fallo secundario (CVE-2026-57221), cualquier usuario autenticado en un Virtual Host (incluso cuentas sin privilegios o de aislamiento básico) puede invocar operaciones pasivas como queue.declare y exchange.declare adivinando o enumerando nombres de recursos. Al saltarse la verificación obligatoria de perfiles, el sistema le revela estadísticas transaccionales detalladas (conteos de mensajes en espera y consumidores conectados) pertenecientes a otros inquilinos (tenants) alojados en el mismo servidor.
- Estado de explotación: No se han reportado incidentes de explotación activa antes de su divulgación pública. Ambos defectos fueron descubiertos por el equipo de investigación de Miggo utilizando su plataforma de auditoría automatizada basada en agentes inteligentes VulnHunter.

Impacto potencial:

- Secuestro absoluto del Bróker de Mensajería corporativo: Al extraer con éxito el secreto criptográfico OAuth de la API expuesta, los atacantes adquieren la capacidad de suplantar legítimamente al bróker de cara al proveedor de identidad institucional. La falsificación les permite emitir credenciales administrativas con las cuales pueden tomar el control de la totalidad del servicio, manipular usuarios, alterar políticas operativas globales del clúster y comprometer los flujos críticos de TI.
- Acceso, inyección y sabotaje de mensajes transaccionales: Al consolidar un perfil administrativo malicioso, el agente de amenaza obtiene facultades ilimitadas de lectura y escritura en los canales de comunicación de RabbitMQ. Esto se traduce en el potencial de interceptar datos bancarios, interceptar eventos lógicos internos, inyectar cargas útiles maliciosas orientadas a aplicaciones cliente downstream, purgar colas completas de peticiones o manipular datos en tránsito relacionados con operaciones comerciales sensibles.
- Fuga de inteligencia empresarial y reconocimiento pasivo en red: El abuso de la enumeración de metadatos multi-inquilino (CVE-2026-57221) dota a los atacantes de una visibilidad profunda sobre la arquitectura lógica de la organización. Al medir los picos en el volumen de mensajes y los consumidores activos de colas ajenas a su perfil, un adversario puede deducir flujos de trabajo específicos de la compañía, identificar qué aplicaciones soportan mayor carga de datos y mapear los nombres internos de los servicios perimetrales para diseñar ataques dirigidos dirigidos a otros segmentos de la red interna.
- Ruptura de los límites de aislamiento Multi-Inquilino (Multi-Tenancy): Las organizaciones que consolidan recursos en la nube asignando aplicaciones de distintos clientes, departamentos o proveedores externos dentro de una única infraestructura compartida de RabbitMQ quedan expuestas a un fallo de confianza colateral. Al saltarse la segregación de seguridad nativa de los Virtual Hosts compartidos, los usuarios maliciosos de un inquilino de prueba o de baja confianza pueden husmear y perfilar la actividad comercial de entornos altamente confidenciales contiguos.

Recomendaciones de mitigación:

1. Actualización obligatoria de RabbitMQ: Actualizar a las versiones 4.3.0, 4.2.6, 4.1.11, 4.0.20 o 3.13.15, las cuales eliminan el endpoint vulnerable GET /api/auth y sustituyen la entrega de parámetros O Auth por un mecanismo interno cifrado durante el proceso de *bootstrap* autenticado. Asimismo, actualizar las imágenes de contenedor utilizadas en producción, los gráficos de Helm y las dependencias de RabbitMQ embebidas en otros productos de la infraestructura para evitar la permanencia de componentes vulnerables.
2. Rotación mandatoria de los secretos de cliente OAuth corporativos: Debido a que la aplicación de parches corrige la vulnerabilidad de software pero no invalida ni revoca información confidencial que pudo haber sido comprometida con anterioridad por métodos de escaneo pasivos, se instruye a los administradores a generar de inmediato nuevas claves secretas en su proveedor de identidad institucional (ej. Keycloak, Microsoft Entra ID) para todos los clústeres donde la directiva management.oauth_client_secret estuviera activa y el puerto de gestión expuesto.
3. Restricción perimetral del plano de gestión (Puerto 15672): Configurar firewalls y grupos de seguridad para bloquear el acceso al puerto 15672 desde Internet, permitiendo únicamente conexiones desde subredes internas de administración, VPN corporativas autorizadas o terminales de bastión (*jump boxes*).
4. Migración hacia esquemas OAuth públicos (PKCE) y segregación estricta de inquilinos: Se recomienda adoptar la arquitectura técnica recomendada de RabbitMQ consistente en implementar flujos de clientes públicos mediante extensiones PKCE (Proof Key for Code Exchange), los cuales por diseño eliminan la necesidad operativa de almacenar y transmitir secretos de cliente estáticos sobre canales HTTP. Asimismo, como contención inmediata ante fallos de enumeración, se debe forzar el aislamiento físico o lógico completo de los datos separando estrictamente a los inquilinos empresariales en instancias independientes de Virtual Hosts que no compartan un plano relacional de usuarios.

Prioridad: Crítica.

Ampliar información:

- https://foro3d.com/2026/julio/fallos-en-rabbitmq-exponen-secretos-oauth-y-datos-de-colas.html
- https://thehackernews.com/2026/07/rabbitmq-flaws-could-leak-oauth-secrets.html
- https://www.csoonline.com/article/4196093/rabbitmq-flaws-expose-oauth-secrets-risk-complete-takeover-of-the-broker.html
- https://www.securityweek.com/rabbitmq-vulnerability-threatens-enterprise-systems/
- https://abit.ee/en/cybersecurity/vulnerabilities/rabbitmq-oauth-vulnerability-cve-message-broker-api-security-en

MALWARE

OKOBOT – MALWARE FRAMEWORK MODULAR DE ALTA SOFISTICACIÓN (INYECCIÓN DE PHISHING Y COMPROMISO DE BILLETERAS CRIPTOGRÁFICAS EN WINDOWS)

Se ha emitido un informe de inteligencia detallado por parte del equipo GReAT de Kaspersky que expone las operaciones activas y la evolución del framework de malware modular de alta sofisticación denominado OkoBot. Esta amenaza, activa en entornos Windows, ha sido diseñada con una arquitectura avanzada de múltiples etapas orientada al espionaje y la exfiltración masiva de activos financieros, credenciales de inicio de sesión y secretos corporativos. El peligro crítico de este framework radica en su módulo especializado SeedHunter, el cual es capaz de interceptar aplicaciones de escritorio legítimas y engañar a los usuarios para sustraer las frases de recuperación física de sus criptoactivos.

OkoBot opera como una plataforma de distribución de payloads orquestada de forma encubierta a través de túneles inversos. A diferencia de los troyanos convencionales, este framework altera dinámicamente la memoria de los procesos del sistema operativo y de los navegadores web para inyectar extensiones ocultas y paneles de control fraudulentos dentro de interfaces de software que gozan de la total confianza del usuario. Con más de 20 complementos identificados, la infraestructura de OkoBot se mantiene en constante mantenimiento y actualización por parte de sus desarrolladores, representando una brecha de seguridad severa para estaciones de trabajo corporativas, entornos de desarrollo de TI y administradores de activos digitales.

Resumen técnico:

- Nombre de la amenaza: OkoBot Framework (asociado al descargador inicial TookPS, el inyector HDUtil y módulos de espionaje avanzados).
- Tipo de vector: Framework de malware persistente, modular y de múltiples etapas (Stealer, Spyware, Keylogger y Backdoor).
- Sistemas afectados: Microsoft Windows de 64 bits, afectando directamente a usuarios de billeteras Ledger Live, Trezor Suite, Exodus, MetaMask y Tonkeeper**,** gestores de credenciales 1Password y KeePassXC**,** y navegadores basados en Chromium como Google Chrome y Microsoft Edge**.**
- Vectores de infección: Se propaga principalmente mediante dos técnicas combinadas: ataques de ingeniería social tipo ClickFix (donde páginas web de falsos CAPTCHAs o actualizaciones engañosas inducen al usuario a ejecutar comandos maliciosos de PowerShell en su consola de comandos) y la distribución de instaladores de software de TI troyanizados en repositorios de GitHub con alto posicionamiento en motores de búsqueda (por ejemplo, guías de instalación falsas de SQL Server Management Studio - SSMS que descargan el editor Audacity compilado con librerías maliciosas integradas).
- Mecanismo de evasión y persistencia: Tras ejecutar TookPS, el malware instala un servicio SSH para crear un túnel inverso hacia el atacante, desactiva alertas de Windows Defender, modifica termsrv.dll para habilitar múltiples sesiones RDP, se agrega al grupo Remote Desktop Users y crea la tarea programada Apple Sync para restablecer el túnel SSH cada hora. Los módulos posteriores, protegidos con VMProtect, implementan evasión del Control de Cuentas de Usuario (UAC) mediante llamadas RPC del sistema operativo.
- Inyección y phishing en aplicaciones (SeedHunter): El malware monitoriza procesos y, al detectar aplicaciones Electron como Trezor Suite **o** Ledger Live**,** inyecta código en sus hilos de ejecución. Cuando identifica una billetera Ledger o Trezor conectada por USB (VID/PID), superpone una interfaz falsa de recuperación de semilla idéntica a la original para capturar las 12 o 24 palabras de recuperación. Las credenciales son interceptadas en texto plano mediante mal_LogConsoleMessage y exfiltradas cifradas con RC4**.**

Impacto potencial:

- Robo masivo de activos digitales mediante exfiltración de frases semilla (Seed Phrases): El compromiso del proceso interno de Ledger Live o Trezor Suite anula la efectividad de las protecciones físicas del hardware. Al capturar las palabras de respaldo directamente en el teclado de la computadora, los atacantes adquieren el control criptográfico maestro de las claves privadas en la blockchain. Esto les faculta para vaciar de manera remota e inmediata la totalidad de los fondos, tokens y activos desde cualquier otra ubicación, volviendo inútil el uso posterior del dispositivo físico comprometido.
- Espionaje audiovisual continuo y filtración de secretos mediante OkoSpyware: El módulo espía OkoSpyware realiza un monitoreo heurístico de más de 100 ejecutables del sistema (billeteras, bóvedas de claves y aplicaciones financieras). Al abrirse cualquiera de estas ventanas, el malware invoca una instancia oculta de la utilidad FFmpeg para grabar en video de formato MP4 las acciones en pantalla del usuario de forma concurrente con el registro de pulsaciones de teclado, comprometiendo visualmente contraseñas maestras, llaves privadas en pantalla y datos confidenciales de navegación.
- Pérdida de control del Endpoint y establecimiento de backdoors de RDP interactivos: La modificación de la librería estructural termsrv.dll y la creación de la tarea persistente de túnel de red conceden a los operadores de OkoBot un acceso de nivel de administrador permanente a la estación de trabajo. La máquina queda expuesta como una pasarela interactiva que permite a los atacantes conectarse en cualquier momento mediante Escritorio Remoto sin interrumpir la sesión visual del usuario legítimo, facilitando el reconocimiento interno de la intranet y la instalación de payloads secundarios de ransomware.
- Exfiltración de credenciales corporativas, cookies de sesión y datos del portapapeles: A través de los plugins integrados y del keylogger avanzado MC Keylogger, el framework extrae sistemáticamente bases de datos de cookies de sesión activa de los navegadores, perfiles de usuario y credenciales guardadas en caché. Adicionalmente, el monitoreo constante de los formatos de portapapeles del sistema operativo (CF_HDROP, CF_UNICODETEXT) captura en tiempo real cualquier contraseña copiada, archivos arrastrados entre directorios corporativos o capturas de pantalla tomadas de forma cíclica cada 5 minutos.

Recomendaciones de mitigación:

1. Auditoría forense activa de persistencias y purga de artefactos en el sistema: Implementar búsquedas centralizadas y reglas de detección en los endpoints (EDR/SIEM) enfocadas en erradicar los elementos característicos dejados por el framework: eliminar de inmediato cualquier tarea programada en el sistema denominada Apple Sync; escanear de manera exhaustiva el almacenamiento local en busca de la presencia de ejecutables en rutas no estándar como %PROGRAMDATA%\HDVideo\HDUtil.exe,%PROGRAMDATA%\hwid.dat,%APPDATA%\hwid.dat y rastros intermedios alojados en %TEMP%\extl.exe o archivos con patrón sh_*.json y media_*. Asimismo, verificar la integridad de la firma digital de la librería termsrv.dll en el directorio System32 contra los archivos originales de Microsoft.
2. Control de membresías de grupos de Windows y bloqueo de tráfico SSH saliente: Inspeccionar periódicamente el grupo local "Usuarios de escritorio remoto" (Remote Desktop Users) para identificar y eliminar cuentas creadas de forma anómala. Complementariamente, configurar políticas restrictivas en firewalls de host o perimetrales para bloquear e interceptar conexiones SSH salientes (Puerto 22 y otros puertos utilizados para túneles) desde estaciones de trabajo que no requieran acceso administrativo.
3. Inspección de perfiles Chromium y control de extensiones: Auditar los perfiles de Google Chrome y Microsoft Edge para detectar extensiones maliciosas ocultas en Local Extension Settings**,** utilizadas por OkoBot para inyectar *stealers* como Rilide**.** Aplicar GPO con listas de extensiones permitidas (*Allowlists*) firmadas corporativamente y bloquear la instalación de archivos .crx externos.
4. Educación sobre Hardware Wallets y vectores ClickFix: Capacitar al personal con acceso a activos digitales o entornos de desarrollo para que identifique que Ledger y Trezor nunca solicitan ingresar la frase semilla mediante el teclado o formularios web; esta debe introducirse exclusivamente desde los botones físicos de la billetera. Además, entrenar a los usuarios para reconocer y reportar ataques ClickFix (ejecución de comandos copiados al portapapeles tras falsas alertas) y restringir la instalación de herramientas de desarrollo desde repositorios externos de GitHub que no hayan sido homologados y revisados.

Prioridad: Urgente.

Ampliar información:

- https://blog.gridinsoft.com/okobot-seed-phrase-malware/
- https://www.scworld.com/brief/okobot-malware-targets-hardware-wallet-users-with-recovery-phrase-phishing
- https://www.kaspersky.com/about/press-releases/kaspersky-reveals-a-new-malicious-framework-targeting-cryptocurrency-users-with-the-use-of-okospyware
- https://securelist.com/okobot-framework-targets-cryptocurrency-wallets/120660/
- https://thehackernews.com/2026/07/okobot-malware-framework-injects-seed.html

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

MICROSOFT PUBLICA EL PATCH TUESDAY MÁS GRANDE DE SU HISTORIA (RÉCORD DE 622 VULNERABILIDADES CORREGIDAS Y DOS ZERO-DAYS BAJO EXPLOTACIÓN ACTIVA)

Microsoft ha desplegado el paquete de actualizaciones mensuales de seguridad (Patch Tuesday) más masivo registrado hasta la fecha correspondiente a julio de 2026, corrigiendo un total sin precedentes de 622 vulnerabilidades únicas de software (570 según la contabilidad del MSRC, ajustadas por componentes duplicados). Este volumen triplica los promedios históricos habituales de la compañía (que rondaban las 200 fallas mensuales). El incremento exponencial en el descubrimiento de brechas de seguridad ha sido atribuido formalmente por el fabricante al uso extensivo de plataformas internas de análisis de código fuente y escaneo predictivo asistidas por Inteligencia Artificial (como el sistema agentic multimódulo MDASH), marcando un nuevo hito operativo en la velocidad de detección y obligando a las organizaciones a reestructurar sus estrategias tradicionales de gestión de parches.

Dentro de esta masiva ventana de actualización, destaca la corrección de urgencia de dos vulnerabilidades de día cero (Zero-Day) que están siendo explotadas activamente por actores de amenazas en entornos reales para comprometer infraestructuras corporativas críticas de colaboración e identidad. Asimismo, el paquete consolida la desactivación forzada y definitiva de compatibilidad para algoritmos heredados e incluye un total de 59 fallas catalogadas como críticas, de las cuales 95 corresponden a vectores de Ejecución Remota de Código (RCE) distribuidos a lo largo del ecosistema Windows, Office y herramientas de desarrollo.

Resumen técnico:

- Métricas globales del ciclo: 622 CVEs únicos corregidos. Se distribuyen en 416 fallas dentro del core de Windows (incluyendo un RCE crítico en VMSwitch registrado como CVE-2026-57092 con CVSS de 9.9), 82 vulnerabilidades en la suite Office, 46 en Microsoft Edge, 27 en herramientas de desarrollo (Visual Studio / Copilot) y 17 específicas de SharePoint Server.
- Zero-Day Activo 1 (SharePoint Server - CVE-2026-56164): Una vulnerabilidad de elevación de privilegios (EoP) explotada a través de la red de manera remota por un atacante no autenticado, sin requerir interacción del usuario ni credenciales previas. Fue detectada en incidentes reales por equipos tácticos de Mandiant y Google FLARE. Coincide críticamente con la fecha de finalización del soporte extendido para SharePoint Server 2016 y 2019, plataformas que carecen de programas de Actualizaciones de Seguridad Extendidas (ESU) de pago.
- Zero-Day Activo 2 (AD FS - CVE-2026-56155): Un fallo de elevación local de privilegios detectado en producción por la unidad DART de Microsoft. Permite a un atacante que ya posee acceso autenticado limitado (por ejemplo, mediante una cuenta de empleado comprometida por phishing) evadir los controles de acceso débiles de Active Directory Federation Services (AD FS) para escalar privilegios a nivel de administración sobre el servidor que firma los tokens de inicio de sesión único (SSO) de toda la organización.
- Fin de la fase de tolerancia para Kerberos RC4: La actualización elimina por completo el interruptor de reversión técnica RC4DefaultDisablementPhase. A partir de este ciclo, el cifrado Kerberos RC4 queda inhabilitado de forma estricta a nivel de sistema operativo y solo operará en cuentas configuradas explícitamente de forma manual, bloqueando las solicitudes de autenticación de cualquier cuenta de servicio residual que no haya migrado a llaves AES.

Impacto potencial:

- Compromiso perimetral y backdoor persistente en SharePoint locales: Al ser el CVE-2026-56164 un vector remoto y no autenticado, los atacantes pueden automatizar escaneos masivos dirigidos a servidores SharePoint auto-hospedados expuestos a internet. Al explotar la elevación de privilegios, toman el control del repositorio documental corporativo, exfiltran patentes, contratos y archivos confidenciales, e inyectan web shells perimetrales capaces de evadir el monitoreo tradicional al operar dentro del contexto de un servicio web legítimo.
- Secuestro de la infraestructura de identidad y Single Sign-On corporativo: La explotación exitosa del fallo en AD FS (CVE-2026-56155) otorga a los atacantes el control sobre el nodo central encargado de validar y emitir las afirmaciones de identidad criptográficas (claims) de la empresa. Un adversario con privilegios administrativos en AD FS puede falsificar tokens de autenticación para cualquier usuario institucional, saltándose por completo los controles perimetrales de doble factor (MFA) para ingresar de manera encubierta a servicios en la nube (Microsoft 365, AWS, SAP) conectados al SSO.
- Caídas operativas masivas y bloqueos de autenticación por Kerberos RC4: Aquellas organizaciones que ejecuten la actualización de julio de 2026 sin realizar una auditoría previa de su Directorio Activo sufrirán denegaciones de servicio internas inmediatas. Las cuentas de servicio de bases de datos, aplicaciones legadas, sistemas CRM heredados o clientes antiguos que sigan solicitando tickets Kerberos basados en RC4 verán denegadas sus solicitudes de inicio de sesión de forma automática, provocando interrupciones operativas críticas y caídas en cadena de aplicaciones productivas a partir de las 2:00 a. m. del despliegue.
- Saturación de los equipos de TI y aumento de la ventana de exposición ("Patch Fatigue"): Administrar un flujo de más de 600 correcciones en un solo mes satura las capacidades de validación, testing y control de cambios de los equipos de infraestructura. Esta sobrecarga de trabajo suele provocar que las organizaciones posterguen el despliegue de parches calificados con severidades CVSS intermedias (como el propio zero-day de SharePoint calificado inicialmente bajo parámetros bajos). Los atacantes aprovechan esta "fatiga de parches" para realizar ingeniería inversa a las actualizaciones mensuales (patch diffing) y diseñar.

Recomendaciones para mitigar el riesgo:

1. Parcheo de máxima urgencia para SharePoint locales y AD FS: Aislar e instalar de manera prioritaria las actualizaciones correspondientes a los dos días cero bajo explotación activa en el inventario tecnológico. Se debe dar prelación absoluta a los servidores físicos o virtuales que ejecuten SharePoint Server (debido a su alcance de red no autenticado) y, de forma contigua, a todos los controladores de dominio y servidores dedicados que alojen el rol de Active Directory Federation Services (AD FS).
2. Despliegue preventivo de protección AMSI en SharePoint Server: Como contención técnica inmediata para mitigar los intentos de explotación dirigidos al CVE-2026-56164 mientras se coordinan las ventanas de mantenimiento y reinicio de los parches de SharePoint locales, se instruye a los administradores a habilitar de forma obligatoria la interfaz de detección Anti-Malware Scan Interface (AMSI) en "Full Mode" en la configuración del servidor, permitiendo inspeccionar las solicitudes dinámicas HTTP entrantes.
3. Ejecutar auditoría Kerberos previa a la actualización y rotación de llaves AES: Antes de desplegar el paquete de parches acumulativos de Windows, es mandatorio auditar las bitácoras del Directorio Activo utilizando los eventos de telemetría de RC4 introducidos a principios de año para identificar qué cuentas de servicio siguen negociando algoritmos inseguros. Una vez identificadas, se debe forzar la rotación de sus contraseñas bajo configuraciones modernas para obligar a Windows a generar e implementar llaves de cifrado avanzadas AES-128/256, resolviendo las dependencias legadas antes de que el interruptor de tolerancia sea eliminado.
4. Priorizar parches según explotación real (KEV/EPSS): Sustituir el triaje basado únicamente en CVSS por un modelo que priorice vulnerabilidades con evidencia de explotación activa. Automatizar la priorización cruzando el inventario de activos con el catálogo KEV de CISA, las métricas EPSS y los indicadores de explotación activa publicados por los fabricantes, ya que vulnerabilidades con puntuaciones CVSS intermedias también son utilizadas en ataques dirigidos.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/07/microsoft-patches-record-622-flaws.html
- https://www.codigovigia.com/blog/ciberseguridad-2/patch-tuesday-julio-2026-570-fallas-record-1069
- https://www.ad-hoc-news.de/boerse/news/ueberblick/microsoft-bate-su-propio-record-de-parches-de-seguridad-en-la-recta-final/69781470#google_vignette
- https://www.brodersendarknews.com/p/microsoft-rompio-el-record-de-vulnerabilidades
- https://es.martincid.com/tecnologia/microsoft-patch-tuesday-july-2026-ai-570-security-flaws/