GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2926

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	1	2	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

CVE-2026-42533 – F5 NGINX (DESBORDAMIENTO DE BÚFER DE MONTÓN Y POSIBLE EJECUCIÓN REMOTA DE CÓDIGO)

Se ha divulgado una vulnerabilidad crítica que afecta al motor de evaluación de expresiones de NGINX, el servidor web y proxy inverso ampliamente utilizado en arquitecturas de red y contenedores. El fallo, identificado como CVE-2026-42533, consiste en un desbordamiento de búfer en el montón (heap buffer overflow) que permite a un atacante remoto no autenticado enviar peticiones HTTP maliciosas diseñadas para provocar la caída recurrente del proceso de trabajo (worker) o, en escenarios avanzados, lograr la ejecución remota de código (RCE) sin requerir credenciales ni interacción del usuario.

Dado que NGINX opera comúnmente en el perímetro de la infraestructura como balanceador de carga, Ingress Controller en Kubernetes o Gateway API, su compromiso expone de manera directa a los servicios y aplicaciones internas alojadas en la red corporativa.

Resumen técnico:

- Identificador principal: CVE-2026-42533.
- Severidad: Crítica / Alta (Puntaje base de 9.2 bajo el estándar CVSS v4.0 y 8.1 bajo CVSS v3.1).
- Causa raíz: Desbordamiento de búfer de montón (Heap Buffer Overflow / CWE-122) originado por un error lógico en la evaluación de dos fases que ejecuta el motor de scripts de NGINX al procesar expresiones dinámicas.
- Mecanismo de falla: El fallo se desencadena bajo una configuración específica donde una directiva map basada en expresiones regulares (regex) devuelve una variable que es posteriormente concatenada o referenciada en una cadena junto a una captura numerada ($1, $2) proveniente de una regla regex previa (como un bloque location). El motor evalúa la Petición en dos pasos: en el primero mide el tamaño necesario y asigna el búfer; en el segundo escribe los datos. Sin embargo, la evaluación del map entre ambas fases sobrescribe el estado compartido de las capturas, provocando que la segunda pasada escriba más datos de los previstos en un búfer sobredimensionado o insuficiente, sobrescribiendo la memoria del heap.
- Estado de explotación: Sin registro formal en el catálogo KEV de CISA al momento del reporte público, pero con pruebas de concepto funcionales en laboratorios de investigación que demuestran la capacidad de filtrar direcciones de memoria no inicializadas para evadir la protección ASLR en sistemas como Ubuntu 24.04. Se anticipa la publicación de exploits públicos a corto plazo.
- Versiones afectadas: Todas las versiones de NGINX Open Source desde la 0.9.6 hasta la 1.31.2 (un rango de código presente desde 2011), NGINX Plus (versiones anteriores a 37.0.3.1), así como las soluciones NGINX Ingress Controller, Gateway Fabric, App Protect WAF e Instance Manager.

Impacto potencial:

- Denegación de servicio (DoS) continua e inestabilidad de la plataforma: Un atacante puede enviar solicitudes HTTP manipuladas que colapsen repetidamente los procesos worker de NGINX. Aunque el sistema operativo reinicia automáticamente los procesos, un flujo constante de ataques genera un bucle de caídas que degrada o interrumpe por completo la disponibilidad de los servicios web.
- Ejecución remota de código (RCE) sin autenticación: En entornos donde la protección de aleatorización del espacio de direcciones (ASLR) esté desactivada, o mediante técnicas de filtrado de memoria del heap que permitan evadirla, el atacante puede tomar el control del proceso de NGINX y ejecutar comandos arbitrarios con los privilegios del usuario del sistema operativo (www-data u homologo).
- Compromiso y exposición de servicios backend enrutados: Al encontrarse NGINX en la frontera perimetral, la toma de control del servidor permite interceptar el tráfico de aplicaciones internas, manipular peticiones entrantes/salientes, exfiltrar encabezados de autenticación y pivotar hacia microservicios restringidos en la red interna o clústeres de Kubernetes.
- Fuga de datos confidenciales residentes en memoria de trabajo: La manipulación del estado de las capturas también permite forzar lecturas anómalas en el heap, retornando fragmentos de memoria no inicializada al atacante a través de respuestas HTTP, lo que facilita la exfiltración de direcciones internas, tokens de sesión de otros usuarios o claves de cifrado en tránsito.

Recomendaciones de mitigación:

1. Aplicación inmediata de las actualizaciones oficiales de NGINX: Actualizar de manera prioritaria las instancias de NGINX Open Source a la versión 1.30.4 (rama estable) o 1.31.3 (rama mainline), y las instalaciones corporativas a NGINX Plus 37.0.3.1. Es indispensable auditar y actualizar de forma independiente los binarios integrados en imágenes de contenedores, pods de Kubernetes e Ingress Controllers.
2. Migración temporal de capturas numeradas a capturas con nombre en archivos de configuración: Si la aplicación de parches no puede realizarse de forma inmediata, se deben revisar las reglas de configuración para reemplazar las capturas numeradas ($1, $2) por capturas con nombre ((?<nombre>...)) dentro de los bloques map y set afectados, reduciendo sustancialmente la superficie expuesta.
3. Auditoría automatizada de sintaxis y directivas en archivos .conf: Desplegar herramientas de escaneo de código o scripts de revisión sobre los archivos de configuración de NGINX para identificar patrones vulnerables (uso de directivas map combinadas con referencias de capturas en set o rewrite), asegurando la corrección de todos los archivos incluidos (include).
4. Endurecimiento perimetral mediante WAF y monitoreo de logs de procesos: Configurar reglas de inspección en el Firewall de Aplicaciones Web (WAF) para bloquear peticiones con estructuras de encabezado anómalas y establecer alertas en el SIEM ante incrementos inusuales en los reinicios de procesos worker o errores de segmentación (segmentation fault) registrados en /var/log/nginx/error.log.

Prioridad: Crítica.

Ampliar información:

- https://blog.sied.ar/2026/07/vulnerabilidad-critica-en-nginx-permite-dos-y-posible-ejecucion-de-codigo-remoto.html
- https://thehackernews.com/2026/07/critical-nginx-vulnerability-can-crash.html
- https://blog.elhacker.net/2026/07/grave-vulnerabilidad-en-f5-nginx-podria.html
- https://www.ingenieriatelematica.com.co/alerta-critica-en-nginx-cve-2026-42533-permite-dos-y-ejecucion-remota-de-codigo/

CVE-2026-8933 – UBUNTU SNAP-CONFINE (ESCALAMIENTO LOCAL DE PRIVILEGIOS)

Se ha divulgado una vulnerabilidad de alta gravedad que afecta a snap-confine, un componente interno del servicio snapd encargado de construir el entorno aislado (sandbox) para aplicaciones empaquetadas en formato Snap dentro de distribuciones Linux. La falla, identificada como CVE-2026-8933, permite a un usuario local sin privilegios elevar sus accesos hasta obtener control total como superusuario (root) en instalaciones por defecto de Ubuntu Desktop. Este vector representa un riesgo significativo para estaciones de trabajo corporativas, equipos de desarrollo y puestos de administración.

Resumen técnico:

- Identificador principal: CVE-2026-8933.
- Severidad: Alta (Puntaje base de 7.8 bajo el estándar CVSS v3.1 - Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Condición de carrera (Race Condition / CWE-362) introducida durante un rediseño de endurecimiento de seguridad en el proceso de inicialización del contenedor aislado.
- Mecanismo de falla: En versiones recientes de Ubuntu, snap-confine crea archivos temporales en /tmp antes de transferir su propiedad a root, lo que permite explotar dos condiciones de carrera: (1) montar un sistema de archivos FUSE para evitar el aislamiento del *sandbox* y (2) usar symlinks para modificar archivos críticos del sistema. Finalmente, al inyectar un archivo malicioso en /run/udev/rules.d/, systemd-udevd ejecuta comandos arbitrarios con privilegios de root.Estado de explotación: Identificado y publicado formalmente por la Unidad de Investigación de Amenazas (TRU) de Qualys. Aunque requiere acceso local previo en el sistema operativo y no es explotable directamente vía red, se han publicado pruebas de concepto técnicas plenamente funcionales.
- Versiones afectadas: Instalaciones por defecto de Ubuntu Desktop 24.04 LTS, 25.10 y 26.04 LTS que ejecuten versiones del paquete snapd anteriores a la 2.76.1 (así como builds no parcheados en versiones LTS con soporte extendido ESM).

Impacto potencial:

- Escalamiento local de privilegios (LPE) a root: Un usuario autenticado con permisos limitados o un proceso comprometido puede obtener control administrativo total del sistema.
- Evasión de AppArmor: La explotación elude las restricciones de AppArmor mediante la manipulación de reglas de udev en /run/udev/rules.d/.
- Compromiso de estaciones de trabajo y entornos de desarrollo: Equipos con Ubuntu Desktop quedan expuestos a la instalación de backdoors, alteración del sistema de archivos y extracción de credenciales o claves SSH.
- Ejecución arbitraria de comandos: La manipulación de systemd-udevd permite ejecutar scripts o binarios con privilegios de root durante eventos del sistema.

Recomendaciones de mitigación:

1. Actualización inmediata del paquete snapd mediante repositorios oficiales: Desplegar de forma prioritaria la versión parcheada de snapd (2.76.1 o superior, o las versiones empaquetadas 2.76+ubuntu22.04.1, 2.76+ubuntu24.04.1 y 2.76+ubuntu26.04.3) ejecutando los comandos sudo apt update && sudo apt install --only-upgrade snapd.
2. Inventario y verificación de versiones de snapd en los endpoints: Validar la versión instalada en cada equipo Linux de la organización ejecutando snap --version o mediante herramientas de gestión de activos (CSAM/EDR), sin asumir que parches genéricos del kernel o la antigüedad de la distribución garantizan la mitigación.
3. Restricción de ejecución de software no confiable a nivel local: Reforzar las políticas de seguridad en endpoints limitando la ejecución de binarios o scripts no firmados descargados por usuarios en /tmp o directorios personales (/home), reduciendo la probabilidad de que un atacante obtenga el primer punto de apoyo (foothold).
4. Monitoreo de eventos del sistema de archivos y reglas de udev: Configurar reglas de auditoría con auditd o agentes EDR para detectar la creación inusual de enlaces simbólicos en /tmp, montajes FUSE no autorizados por usuarios no privilegiados y la escritura de archivos en el directorio /run/udev/rules.d/.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/07/ubuntu-snap-confine-flaw-could-give.html
- https://blog.qualys.com/vulnerabilities-threat-research/2026/07/21/cve-2026-8933-snap-confine-local-privilege-escalation
- https://blog.segu-info.com.ar/2026/07/vulnerabilidad-de-escalamiento-en.html
- https://www.mentehackers.com/vulnerabilidad-ubuntu-desktop-acceso-root-abfdd9e7
- https://unaaldia.hispasec.com/un-fallo-en-snap-confine-permite-obtener-root-en-ubuntu-desktop-con-acceso-local/

CVE-2026-48294 – ADOBE ACROBAT CHROME EXTENSION (DIVULGACIÓN DE DATOS ENTRE ORÍGENES Y EXPOSICIÓN DE CHATS EN WHATSAPP WEB)

Se ha revelado una vulnerabilidad de alta gravedad que afecta a la extensión oficial de Adobe Acrobat para Google Chrome y navegadores basados en Chromium, un complemento ampliamente instalado con más de 300 millones de usuarios a nivel global. El fallo, identificado como CVE-2026-48294 y bautizado por investigadores como "HermeticReader", permite a un sitio web malicioso omitir la Política de Mismo Origen (Same-Origin Policy - SOP) del navegador. A través de este vector, un atacante remoto puede exfiltrar de manera silenciosa información confidencial de sesiones activas en otras pestañas, demostrándose el robo directo de chats, contactos y mensajes en WhatsApp Web sin requerir la instalación de malware ni la extracción de credenciales o cookies.

Resumen técnico:

- Identificador principal: CVE-2026-48294 (Denominado "HermeticReader").
- Severidad: Alta (Puntaje base de 7.4 bajo el estándar CVSS v3.1 - Riesgo Alto / Exposición Cross-Origin UXSS).
- Causa raíz: Vulnerabilidad de divulgación de datos entre orígenes de clase Universal Cross-Site Scripting (UXSS) debido a una falta de validación de origen en recursos HTML/iframes internos de la extensión y al uso de permisos excesivamente elevados dentro del navegador.
- Mecanismo de falla: La extensión incorpora un componente interno denominado motor Hermes, diseñado para gestionar la integración de lectura de documentos PDF en WhatsApp Web. Una página web maliciosa puede incrustar un marco oculto (iframe) de los recursos de la extensión y enviar comandos no verificados a su service worker para activar el motor Hermes. Obteniendo el identificador numérico de la pestaña (Tab ID) de WhatsApp Web, el atacante utiliza las capacidades de la extensión para inyectar un formulario en el DOM de WhatsApp Web. Dado que un elemento de opción HTML sin valor envía todo el texto renderizado en su nodo y la política CSP de WhatsApp Web no restringía form-action, la propia pestaña de WhatsApp realiza una petición POST que envía la lista de chats, nombres de contactos y mensajes visibles directamente hacia el servidor del atacante.
- Estado de explotación: Descubierta e informada a Adobe por investigadores de Guardio Labs. Aunque no se registraron ataques masivos en el momento del reporte, la vulnerabilidad afectaba a una base instalada masiva de navegadores y contó con pruebas de concepto (PoC) totalmente funcionales.
- Versiones afectadas: Extensión oficial de Adobe Acrobat para Chrome (ID: efaidnbmnnnibpcajpcglclefindmkaj) en sus versiones 26.5.2.2 y anteriores.

Impacto potencial:

- Fuga de información confidencial y privacidad de comunicaciones: Un usuario que visite un sitio web malicioso teniendo abierta una pestaña de WhatsApp Web expone instantáneamente su historial de chats visibles, nombres de contactos, previas de mensajes y nombre de perfil, comprometiendo la privacidad de las conversaciones personales y corporativas.
- Bypass completo de la Política de Mismo Origen (SOP) del navegador: El abuso de los permisos elevados de la extensión neutraliza el aislamiento de seguridad por pestañas de Chrome, sentando un precedente de riesgo donde sitios no confiables pueden interactuar indirectamente con aplicaciones web autenticadas.
- Riesgo potencial de secuestro de cuenta por sustitución de código QR: Los investigadores demostraron que la capacidad de manipulación sobre el DOM de WhatsApp Web permite modificar el código QR de vinculación de dispositivos en pantalla, pudiendo llevar al secuestro de la cuenta si el usuario escanea un código manipulado.
- Exfiltración de datos corporativos en entornos de teletrabajo: Dado el uso frecuente de WhatsApp Web y la extensión de Adobe Acrobat en equipos de trabajo, el fallo facilita el espionaje corporativo y la fuga de información sensible, documentos e hipervínculos compartidos en conversaciones activas.

Recomendaciones de mitigación:

1. Verificación y actualización de Adobe Acrobat: Confirmar que la extensión de Adobe Acrobat esté actualizada a la versión 26.5.2.3 o superior. Para verificarlo, acceder a chrome://extensions, activar el Modo de desarrollador y forzar la actualización del complemento.
2. Gestión y restricción centralizada de extensiones mediante GPO: Implementar políticas de grupo para auditar, restringir o desinstalar extensiones no esenciales que soliciten permisos de lectura e interacción en todas las páginas web (<all_urls>).
3. Auditoría de sesiones activas y dispositivos vinculados en WhatsApp: Indicar a los colaboradores revisar periódicamente en la aplicación móvil de WhatsApp el apartado "Dispositivos vinculados" y cerrar de inmediato cualquier sesión en navegador desconocida o que ya no se encuentre en uso.
4. Adopción del principio de mínimo privilegio en complementos de navegador: Promover buenas prácticas de navegación que incluyan la eliminación de complementos con bajas garantías de seguridad y el uso de perfiles de navegación separados para tareas administrativas o manejo de mensajería corporativa.

Prioridad: Urgente.

Ampliar información:

- https://thehackernews.com/2026/07/adobe-acrobat-extension-flaw-let.html
- https://www.diarioestrategia.cl/texto-diario/mostrar/5963427/fallo-extension-adobe-acrobat-chrome-permitia-acceder-conversaciones-whatsapp-web
- https://www.ghacks.net/2026/07/23/adobe-patches-acrobat-chrome-extension-flaw-that-exposed-whatsapp-web-chats-to-any-website/
- https://www.heise.de/en/news/Adobe-Chrome-extension-enabled-data-theft-11377090.html
- https://www.redeszone.net/noticias/seguridad/fallo-adobe-acrobat-chrome-chats-whatsapp/
- https://www.infobae.com/tecno/2026/07/23/tus-chats-de-whatsapp-web-podrian-quedar-expuestos-por-una-falla-en-la-extension-de-adobe-acrobat/

MALWARE

HOLLOWGRAPH – FRAMEWORK DE ESPIONAJE MODULAR (ABUSO DE LA API MICROSOFT GRAPH Y CANAL C2 EN CALENDARIOS DE MICROSOFT 365)

Se ha identificado HollowGraph, un implante de espionaje cibernético asociado al framework Cavern, que abusa de la API de Microsoft Graph mediante cuentas o aplicaciones de Microsoft 365 comprometidas. La amenaza utiliza el calendario del buzón como canal encubierto de mando y control (C2), ocultando instrucciones y datos exfiltrados en eventos programados para el año 2050, lo que le permite evadir las herramientas tradicionales de monitoreo y seguridad.

Resumen técnico:

- Nombre de la amenaza: HollowGraph (componente del framework de puerta trasera Cavern, asociado potencialmente a grupos de espionaje del nexo de Irán como Lyceum / OilRig).
- Tipo de vector: Implante de espionaje cibernético y puerta trasera (Backdoor / Data Exfiltration) compilado como una librería DLL en .NET NativeAOT.
- Sistemas y entornos afectados: Organizaciones con despliegues de Microsoft 365, Microsoft Entra ID (anteriormente Azure AD) y servicios integrados mediante la API de Microsoft Graph.
- Mecanismo de operación y C2: El malware utiliza dos comandos (get y send). Para recibir tareas, consulta el calendario del buzón comprometido en busca de eventos creados por el atacante (13 de mayo de 2050) y lee las instrucciones desde archivos adjuntos. Para exfiltrar información, cifra los datos robados y crea eventos futuros con adjuntos (File{n}.txt). La comunicación está protegida mediante cifrado híbrido RSA-OAEP y AES-256-GCM con claves independientes para recepción y envío.
- Persistencia y canal DNS de respaldo: Para mantener el acceso y refrescar las credenciales de Entra ID (ID de inquilino, ID de cliente y secreto de cliente), HollowGraph utiliza un canal independiente de tunelización DNS. El implante envía consultas AAAA de IPv6 hacia cloudlanecdn[.]com, decodifica las credenciales recibidas y las almacena localmente en logAzure.txt.

Impacto potencial:

- Exfiltración silenciosa de información altamente confidencial: Al utilizar el calendario de Microsoft 365 como buzón muerto cifrado, los atacantes pueden extraer documentos, archivos y secretos corporativos sin activar alertas en firewalls perimetrales o sistemas de prevención de intrusiones (IPS/IDS).
- Evasión total de los controles de seguridad de red perimetrales: Dado que todas las peticiones C2 principales se realizan mediante conexiones legítimas HTTPS dirigidas a las URLs oficiales de la API de Microsoft Graph, el tráfico malicioso resulta indistinguible de la actividad cotidiana de colaboración de la empresa.
- Persistencia prolongada en la capa de Identidad y SaaS: La capacidad de refrescar de forma encubierta credenciales OAuth y secretos de cliente de Entra ID vía DNS permite al actor de amenazas mantener el control del canal de exfiltración de forma indefinida, incluso si se modifican contraseñas de usuario tradicionales.
- Riesgo de compromiso en la cadena de suministro y plataformas en la nube: Un compromiso exitoso en la cuenta o aplicación con permisos de Microsoft Graph faculta a los atacantes para explorar otros servicios interconectados del ecosistema Microsoft 365 (como SharePoint, OneDrive o contactos), facilitando el espionaje dirigido en la infraestructura corporativa.

Recomendaciones de mitigación:

1. Cacería de amenazas y auditoría de calendarios: Auditar Microsoft 365 y Graph API en busca de eventos programados para el 13 de mayo de 2050, asuntos con GUID o patrones Event ID:/Boss{..}ID{..}, y adjuntos File{n}.txt.
2. Control de aplicaciones OAuth y permisos de Graph: Revisar las aplicaciones en Microsoft Entra ID, aplicar el principio de mínimo privilegio en Graph API y generar alertas ante la creación o modificación de secretos de cliente.

3. Monitoreo de tráfico DNS: Detectar tunelización DNS mediante consultas AAAA de IPv6 o subdominios de alta entropía dirigidos a dominios no verificados como cloudlanecdn[.]com.
4. Monitoreo de identidad y EDR/XDR: Fortalecer el Acceso Condicional, rotar periódicamente los secretos de aplicaciones y utilizar EDR/XDR para detectar comportamientos anómalos y archivos como logAzure.txt.

Prioridad: Urgente.

Ampliar información:

- https://www.helpnetsecurity.com/2026/07/20/hollowgraph-malware-microsoft-365-calendar/
- https://www.uvcyber.com/resources/reports/threat-advisory-hollowgraph-malware
- https://www.broadcom.com/support/security-center/protection-bulletin/hollowgraph-malware-leverages-microsoft-365-calendar-events-for-c2-communication
- https://q2bstudio.com/nuestro-blog/2091730/el-malware-hollowgraph-usa-el-calendario-de-microsoft-365-como-cc
- https://www.ingenieriatelematica.com.co/hollowgraph-malware-oculta-c2-y-archivos-robados-en-calendarios-de-microsoft/
- https://thehackernews.com/2026/07/hollowgraph-malware-hides-c2-and-stolen.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

EXPLOTACIÓN ACTIVA DE VULNERABILIDAD CRÍTICA RCE EN MICROSOFT SHAREPOINT SERVER (CVE-2026-50522) Y ROBO DE LLAVES DE MÁQUINA

Se ha confirmado la explotación activa en entornos reales de una vulnerabilidad crítica de Ejecución Remota de Código (RCE) que afecta a las instalaciones locales (on-premises) de Microsoft SharePoint Server. El fallo, rastreado como CVE-2026-50522, surge a raíz de una deserialización insegura de datos no confiables en el flujo de autenticación del servidor.

Tras la publicación del PoC, múltiples actores de amenazas comenzaron a explotar los endpoints de inicio de sesión de SharePoint (/_trust/default.aspx). Además de la ejecución de comandos arbitrarios, los atacantes buscan robar las IIS Machine Keys para falsificar tokens de autenticación y mantener acceso persistente incluso después de aplicar los parches. Debido a su alto impacto, CISA incluyó esta vulnerabilidad en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV).

Resumen técnico:

- Identificador principal: CVE-2026-50522.
- Severidad: Crítica (Puntaje base de 9.8 bajo el estándar CVSS v3.1 / CVSS v4.0 - Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Causa raíz: Deserialización de datos no confiables (CWE-502) dentro de la clase SessionSecurityTokenHandler de la infraestructura de identidad de .NET en SharePoint.
- Mecanismo de falla: Un atacante remoto no autenticado envía un paquete HTTP manipulado con un objeto serializado (.NET BinaryFormatter) hacia los endpoints de inicio de sesión de SharePoint. Al procesarlo sin validar el tipo de objeto, el servicio ejecuta código arbitrario en el proceso de IIS (w3wp.exe).
- Estado de explotación: Explotación activa confirmada en la práctica a nivel global, con disponibilidad de PoC pública e inclusión oficial en el catálogo KEV de CISA.
- Versiones afectadas: Implementaciones on-premises de Microsoft SharePoint Enterprise Server 2016 (anteriores a 16.0.5561.1001), SharePoint Server 2019 (anteriores a 16.0.10417.20175) y SharePoint Server Subscription Edition (anteriores a 16.0.19725.20434). SharePoint Online (SaaS) no se ve afectado.

Impacto potencial:

- Ejecución remota de código (RCE) sin autenticación: Un atacante no autorizado puede tomar el control absoluto del servidor SharePoint expuesto sin requerir credenciales válidas ni interacción por parte de ningún usuario (Zero-Click).
- Compromiso de credenciales mediante robo de IIS Keys: El robo de las IIS Machine Keys permite al atacante falsificar tokens de sesión y mantener acceso persistente a la plataforma, incluso después de reiniciar el servidor o aplicar los parches de seguridad.
- Despliegue de web shells y movimiento lateral en el dominio corporativo: El acceso con privilegios a nivel de servidor habilita la implantación de web shells para el control remoto persistente y sirve como punto de apoyo inicial (foothold) para pivotar y comprometer controladores de dominio o bases de datos internas.
- Exfiltración y alteración de bases de datos de contenido crítico: Los atacantes pueden extraer información confidencial, documentos restringidos, secretos de aplicaciones e historiales almacenados en las granjas de SharePoint de la organización.

Recomendaciones para mitigar el riesgo:

1. Aplicación inmediata de los parches de seguridad de Microsoft: Desplegar de forma urgente la actualización acumulativa del Patch Tuesday (julio de 2026) en todas las granjas y nodos de SharePoint Server on-premises (KB5002891 para 2016/Subscription Edition y KB5002883 para 2019).
2. Rotación obligatoria de las llaves de máquina (IIS Machine Keys) y secretos: Dado que la aplicación del parche no invalida las llaves robadas previamente por los atacantes, es indispensable llevar a cabo un proceso de auditoría y rotación de las llaves de máquina de IIS y credenciales de cuentas de servicio/granja en todos los servidores expuestos.
3. Restricción del perímetro y aislamiento de servidores SharePoint: Evaluar la exposición pública de los servidores SharePoint locales, ubicándolos detrás de una VPN corporativa, arquitecturas Zero Trust (ZTNA) o un Firewall de Aplicaciones Web (WAF) configurado con reglas de inspección contra payloads de deserialización .NET.
4. Cacería de amenazas (Threat Hunting) e inspección de procesos: Auditar los registros de IIS en busca de peticiones anómalas dirigidas a /_trust/default.aspx y monitorear la creación de procesos secundarios sospechosos (como cmd.exe o powershell.exe) iniciados desde el proceso trabajador w3wp.exe.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2026/07/critical-sharepoint-rce-cve-2026-50522.html
- https://socradar.io/blog/cve-2026-50522-poc-fuels-sharepoint-attacks/
- https://devel.group/blog/ejecucion-remota-de-codigo-no-autenticada-en-servidores-sharepoint-cvss-9-8/
- https://www.ingenieriatelematica.com.co/alerta-vulnerabilidad-critica-rce-en-sharepoint-server-cve-2026-50522-bajo/
- https://www.threatlocker.com/blog/sharepoint-rce-under-active-exploitation
- https://www.helpnetsecurity.com/2026/07/22/sharepoint-cve-2026-50522-exploited/
- https://blog.elhacker.net/2026/07/vulnerabilidad-critica-de-ejecucion.html