GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3725

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	1
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	1	0	0

VULNERABILIDADES

VULNERABILIDAD CRÍTICA EN ADOBE COMMERCE Y MAGENTO OPEN SOURCE (CVE-2025-54236 – "SESSIONREAPER")

El 9 de septiembre de 2025, Adobe publicó un parche de emergencia para corregir una vulnerabilidad crítica en Adobe Commerce y Magento Open Source que permite la toma de control de cuentas de clientes a través de la API REST. La falla, identificada como CVE-2025-54236 y apodada SessionReaper, tiene un puntaje CVSS de 9.1/10. Adobe rompió su ciclo habitual de actualizaciones (previsto para octubre) debido a la alta probabilidad de explotación masiva.

Resumen técnico:

- CVE-2025-54236 (SessionReaper, CVSS 9.1): validación inadecuada de entradas en el componente Web API ServiceInputProcessor, lo que permite pasar parámetros no sanitizados a constructores backend.
- Impacto: un atacante remoto no autenticado puede secuestrar sesiones, tomar control de cuentas de clientes, robar datos y generar pedidos fraudulentos sin necesidad de tokens válidos.
- Productos afectados:
- Adobe Commerce (todas las implementaciones): 2.4.9-alpha2 y anteriores, 2.4.8-p2 y anteriores, 2.4.7-p7 y anteriores, 2.4.6-p12 y anteriores, 2.4.5-p14 y anteriores, 2.4.4-p15 y anteriores.
- Adobe Commerce B2B: 1.5.3-alpha2 y anteriores, 1.5.2-p2 y anteriores, 1.4.2-p7 y anteriores, 1.3.4-p14 y anteriores, 1.3.3-p15 y anteriores.
- Magento Open Source: mismas versiones que Adobe Commerce.
- Custom Attributes Serializable module: 0.1.0 a 0.4.0.
- Explotación: aunque aún no se han confirmado ataques en producción, investigadores de Sansec demostraron la viabilidad de la explotación y se prevé una explotación masiva en corto plazo tras la divulgación.
- Corrección: Adobe liberó parches oficiales el 9 de septiembre y activó reglas de WAF en Adobe Commerce Cloud.

Impacto potencial:

- Compromiso total de cuentas de clientes en plataformas de e-commerce.
- Robo de información personal y financiera.
- Riesgo de explotación automatizada a gran escala, como ocurrió con vulnerabilidades previas (Shoplift 2015, TrojanOrder 2022, CosmicSting 2024).
- Posible encadenamiento con otras fallas para alcanzar ejecución remota de código.
- Riesgo elevado para empresas minoristas y plataformas de comercio electrónico a nivel global.

Recomendaciones de mitigación:

1. Aplicar inmediatamente los parches oficiales liberados por Adobe.
2. Invalidad cookies de sesión y forzar reautenticación de clientes.
3. Rotar credenciales de API y cuentas de servicio.
4. Configurar reglas de WAF con validación estricta de JSON schema para la API REST.
5. Migrar el almacenamiento de sesiones a Redis o base de datos (si aún se utiliza almacenamiento en archivos).
6. Monitorear logs en busca de actividad anómala en el uso de la API.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/09/adobe-commerce-flaw-cve-2025-54236-lets.html
- https://gbhackers.com/sessionreaper-vulnerability/

VULNERABILIDADES CRÍTICAS EN SAP NETWEAVER Y S/4HANA (CVSS HASTA 10.0)

El 9 de septiembre de 2025, SAP publicó actualizaciones de seguridad que corrigen múltiples vulnerabilidades críticas en sus productos NetWeaver y S/4HANA. Entre ellas destacan tres fallas en NetWeaver con impacto de ejecución de código y acceso indebido, así como una vulnerabilidad crítica en S/4HANA que ya se encuentra bajo explotación activa en la naturaleza.

Resumen técnico:

- CVE-2025-42944 (CVSS 10.0, NetWeaver): vulnerabilidad de deserialización en el módulo RMI-P4 que permite a un atacante remoto no autenticado enviar un payload malicioso a un puerto abierto, resultando en ejecución de comandos del sistema operativo.
- CVE-2025-42922 (CVSS 9.9, NetWeaver AS Java): manejo inseguro de archivos que permite a un usuario autenticado sin privilegios de administrador subir archivos arbitrarios al sistema.
- CVE-2025-42958 (CVSS 9.1, NetWeaver IBM i-Series): falta de validación de autenticación que permite a usuarios altamente privilegiados no autorizados leer, modificar o borrar información sensible y acceder a funciones administrativas.
- CVE-2025-42916 (CVSS 8.1, S/4HANA): validación insuficiente que permite a un usuario con altos privilegios en ABAP eliminar tablas de base de datos sin controles adecuados.
- CVE-2025-42957 (CVSS 9.9, S/4HANA): vulnerabilidad de inyección de comandos ABAP vía RFC, reportada en agosto y actualmente bajo explotación activa. Permite a un atacante con credenciales de bajo nivel escalar privilegios, crear cuentas superusuario y comprometer completamente el sistema.

Impacto potencial:

- Compromiso total de entornos SAP NetWeaver y S/4HANA en sectores críticos (finanzas, manufactura, cadena de suministro, recursos humanos).
- Robo o manipulación de datos sensibles, creación de cuentas ocultas y persistencia en el sistema.
- Riesgo de explotación masiva de la vulnerabilidad CVE-2025-42957, ya confirmada como utilizada en ataques dirigidos.
- Posible utilización de estas fallas como punto de entrada para espionaje, fraude corporativo o despliegue de ransomware en infraestructuras críticas.

Recomendaciones de mitigación:

1. Aplicar inmediatamente los parches oficiales publicados por SAP (Patch Day septiembre 2025).
2. Implementar filtrado de puertos P4 en el ICM para reducir superficie de ataque en NetWeaver.
3. Revisar y endurecer permisos de usuarios en SAP, minimizando accesos innecesarios a módulos RFC y ABAP.
4. Monitorear logs de explotación de CVE-2025-42957 e indicadores de persistencia (cuentas superusuario creadas de forma anómala).
5. Segmentar el acceso administrativo y reforzar controles de autenticación en entornos SAP críticos.

Prioridad: Crítica

Ampliar Información:

- https://thehackernews.com/2025/09/sap-patches-critical-netweaver-cvss-up.html
- https://securityaffairs.com/181930/hacking/critical-sap-s-4hana-flaw-cve-2025-42957-under-active-exploitation.html

VULNERABILIDADES CRÍTICAS EN QNAP QVR (VioStor NVR LEGACY) – CVE-2025-52856 Y CVE-2025-52861

El 5 de septiembre de 2025, QNAP publicó un boletín de seguridad alertando sobre dos vulnerabilidades críticas en el componente QVR para VioStor NVR (legacy) que pueden permitir a un atacante remoto pasar de omitir la autenticación a obtener control total del sistema.

Resumen técnico:

- CVE-2025-52856 (Bypass de autenticación): permite a un atacante remoto evadir completamente el sistema de autenticación del firmware QVR, accediendo sin credenciales válidas ni mecanismos de defensa adicionales (ej. MFA).
- CVE-2025-52861 (Path traversal): un atacante con acceso administrativo puede manipular rutas de ficheros (ej. mediante ../) para acceder a información sensible, incluyendo credenciales y configuraciones críticas, posibilitando el compromiso total de la infraestructura.
- Productos afectados: rama QVR VioStor NVR 5.1.x.
- Corrección: actualización a QVR versión 6.1.6 (20250621) o posterior, disponible en el portal oficial de QNAP.

Impacto potencial:

- Acceso no autenticado y remoto a sistemas NAS/NVR expuestos.
- Robo de datos sensibles, incluidas credenciales y configuraciones de red.
- Compromiso total de la infraestructura asociada al dispositivo.
- Riesgo de utilización de los equipos como puerta de entrada para ataques de ransomware o movimientos laterales dentro de la red corporativa.

Recomendaciones de mitigación:

1. Actualizar inmediatamente el firmware de QVR a la versión 6.1.6 (20250621) o superior.
2. Descargar únicamente el firmware desde las URLs oficiales de QNAP.
3. Restringir la exposición de dispositivos QNAP a internet, limitando accesos administrativos a redes seguras.
4. Monitorizar registros en busca de intentos de explotación de autenticación o acceso a rutas indebidas.
5. Segmentar la red para reducir el impacto en caso de compromiso de dispositivos NAS/NVR.

Prioridad: Crítica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/09/vulnerabilidades-criticas-exponen-los-sistemas-qnap.html
- https://cybersecuritynews.com/qnap-authentication-vulnerability/

VULNERABILIDAD EN FORTIDDOS-F – INYECCIÓN DE COMANDOS EN CLI (CVE-2024-45325)

El 9 de septiembre de 2025, Fortinet publicó el aviso FG-IR-24-344 confirmando una vulnerabilidad de inyección de comandos del sistema operativo (OS Command Injection) en FortiDDoS-F, identificada como CVE-2024-45325, con una severidad Media (CVSS 6.5).

Resumen técnico:

- CVE-2024-45325 (CVSS 6.5, CWE-78): inadecuada neutralización de elementos especiales en la interfaz de línea de comandos (CLI).
- Vector de ataque: requiere acceso local con privilegios altos (PR:H). No requiere interacción del usuario.
- Impacto: un atacante autenticado y con privilegios elevados puede ejecutar comandos arbitrarios en el sistema, comprometiendo confidencialidad, integridad y disponibilidad.
- Descubrimiento: vulnerabilidad reportada internamente por Théo Leleu (Fortinet Product Security).

Versiones afectadas:

- FortiDDoS-F 7.0: 7.0.0 a 7.0.2 → actualizar a 7.0.3 o superior.
- FortiDDoS-F 6.6 y anteriores (6.1 – 6.6): todas las versiones vulnerables → migrar a versión corregida.
- FortiDDoS-F 7.2: no afectado.

Impacto potencial:

- Ejecución de comandos arbitrarios en dispositivos de mitigación DDoS.
- Posible compromiso completo del sistema si un atacante obtiene acceso privilegiado.
- Riesgo de que un usuario interno malicioso o atacante que logre escalar privilegios explote la falla.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a FortiDDoS-F 7.0.3 en ramas 7.0.
2. Migrar a versiones corregidas en ramas 6.x (6.1 – 6.6).
3. Restringir accesos locales y privilegiados a la CLI, aplicando el principio de menor privilegio.
4. Implementar monitoreo de logs de CLI para detectar comandos anómalos.

Prioridad: Importante.

Ampliar Información:

- https://cybersecuritynews.com/fortiddos-os-command-injection-vulnerability/
- https://www.tenable.com/cve/CVE-2024-45325

RECOMENDACIONES GENERALES SOBRE VULNERABILIDADES:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Server
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

RATON: TROYANO BANCARIO PARA ANDROID CON ATAQUES NFC Y ATS

El 9 de septiembre de 2025, investigadores de ThreatFabric revelaron la existencia de un nuevo troyano bancario para Android denominado RatOn, que combina ataques de relay NFC con funciones de Remote Access Trojan (RAT) y un Automated Transfer System (ATS), convirtiéndose en una de las amenazas móviles más avanzadas del año.

Resumen técnico:

- Evolución: RatOn surge como evolución del malware NFSkate, incorporando ahora capacidades de relay NFC (Ghost Tap), superposición de pantallas (overlays) y fraude automatizado con transferencias ATS.
- Distribución: se propaga mediante páginas falsas de Google Play Store, presentándose como aplicaciones fraudulentas (ej. “TikTok 18+”).
- Funcionalidades principales:

- Account takeover de aplicaciones financieras y de criptomonedas (ej. MetaMask, Trust, Phantom, Blockchain.com).
- Fraude bancario automatizado (ATS): ejecuta transferencias en la app George Česko (banco en República Checa) sin intervención del usuario.
- Overlay & ransomware-like: despliega pantallas falsas de bloqueo exigiendo pagos en criptomonedas (~200 USD), simulando extorsión por contenido ilegal.
- NFC relay: permite realizar fraudes de pago sin contacto en cajeros o POS.
- Permisos abusivos: solicita accesibilidad, administración de dispositivo y permisos de instalación de apps externas para escalar privilegios.
- Comandos soportados: envío de SMS, grabación de pantalla, bloqueo de dispositivo, inyección en apps financieras, lanzamiento de WhatsApp/Facebook, creación de contactos falsos y ejecución de APKs adicionales.

Impacto potencial:

- Compromiso total de dispositivos Android infectados.
- Robo de credenciales, PINs y frases semilla de billeteras de criptomonedas.
- Ejecución de transferencias fraudulentas de forma automatizada.
- Riesgo de extorsión psicológica a través de overlays con mensajes falsos de delitos graves.
- Expansión regional: primero detectado en República Checa y Eslovaquia, con posibilidad de escalar a otros países europeos.

Recomendaciones de mitigación:

1. Evitar la instalación de aplicaciones desde enlaces externos o tiendas falsas.
2. Restringir permisos de accesibilidad y administración solo a apps legítimas.
3. Implementar soluciones de seguridad móvil (MDM/MAM) en entornos corporativos.
4. Monitorear indicadores de compromiso relacionados con RatOn y NFSkate.
5. Educar a los usuarios sobre fraudes con overlays y extorsión digital.

Prioridad: Urgente

Ampliar Información:

- https://thehackernews.com/2025/09/raton-android-malware-detected-with-nfc.html
- https://www.pcdemano.com/sc/internet/hackers/37036/
- https://nubetia.com/es/raton-el-nuevo-malware-para-android-con-capacidades-de-fraude-bancario-y-ataques-nfc/

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

OLA DE ATAQUES A SALESFORCE Y SU CADENA DE SUMINISTRO

El 3 de septiembre de 2025, Cloudflare confirmó haber sido víctima de un ataque a su instancia de Salesforce CRM, en el marco de una campaña de la cadena de suministro vinculada a Salesloft Drift y atribuida al grupo de extorsión ShinyHunters (UNC6040).

Resumen técnico:

- Vector de ataque: uso de tokens OAuth comprometidos en aplicaciones conectadas a Salesforce (ej. Data Loader), obtenidos mediante tácticas de ingeniería social y phishing de voz (vishing). Los atacantes persuadieron a empleados para vincular aplicaciones OAuth maliciosas con el entorno corporativo.
- Exfiltración: tras una fase de reconocimiento el 9 de agosto, los atacantes extrajeron objetos de Salesforce (Account, Contact, Case y Opportunity) entre el 12 y 17 de agosto, incluyendo 104 tokens de API de Cloudflare y datos textuales de casos de soporte. Parte de esta información contenía credenciales sensibles (tokens, claves, contraseñas). Los atacantes borraron consultas para ocultar evidencias (anti-forensics).
- Otros afectados: Palo Alto Networks y otras empresas confirmaron robo de datos de soporte en Salesforce, incluyendo posibles claves de AWS, cadenas de VPN/SSO y tokens de Snowflake.
- Campaña en curso: ShinyHunters viene atacando instancias de Salesforce desde junio de 2025, usando aplicaciones OAuth maliciosas y exfiltración automatizada vía Bulk API. Se han observado técnicas de scraping de credenciales mediante consultas SOQL y exfiltración masiva con Python/3.11 aiohttp/3.12.15, indicativo de abuso de librerías asíncronas para extracción a gran escala.

Impacto potencial:

- Compromiso de datos sensibles en cientos de organizaciones que usan Salesforce y sus integraciones.
- Reutilización de credenciales y tokens exfiltrados para acceder a otros servicios en la nube (AWS, Snowflake, VPNs, SSO).
- Riesgo de extorsión y chantaje por parte de ShinyHunters, conocido por filtrar datos de grandes compañías (Google, Cisco, AT&T, LVMH, entre otros).

- Aumento del riesgo en la cadena de suministro SaaS, con impacto indirecto en clientes de proveedores como Cloudflare y Palo Alto Networks.

Recomendaciones para mitigar el riesgo:

- Rotar inmediatamente tokens OAuth, API keys y credenciales compartidas en Salesforce.
- Revisar logs de acceso y auditoría en Salesforce (incluyendo Event Monitoring y consultas SOQL ejecutadas) para detectar actividad inusual.
- Buscar IoCs de esta campaña, como el user-agent Python/3.11 aiohttp/3.12.15 y accesos desde nodos Tor.
- Usar herramientas de escaneo de secretos (Trufflehog, GitLeaks) para identificar credenciales potencialmente expuestas en datos exfiltrados.
- Limitar el uso de aplicaciones conectadas y reforzar políticas de Zero Trust y privilegios mínimos.
- Sensibilizar a los empleados sobre ataques de vishing y verificar la legitimidad de cualquier solicitud de integración externa.

Prioridad: Crítica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/09/sigue-la-sangria-de-ataques-sales-force.html
- https://www.bleepingcomputer.com/news/security/cloudflare-hit-by-data-breach-in-salesloft-drift-supply-chain-attack/
- https://unit42.paloaltonetworks.com/threat-brief-compromised-salesforce-instances/