GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3325

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
VULNERABIILIDADES	3	1	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

Vulnerabilidad permite “Compromiso total de dominio” en implementaciones híbridas de Exchange (CVE-2025-53786)

Microsoft ha alertado sobre una grave vulnerabilidad en entornos híbridos de Exchange Server, que puede permitir a un atacante con control del servidor local obtener privilegios administrativos también en Exchange Online, sin dejar rastros visibles en los registros de auditoría.

Resumen técnico:

- El entorno híbrido utiliza una identidad compartida basada en certificado para autenticar entre Exchange On-Premises y Exchange Online.
- Si un atacante compromete el servidor local con privilegios administrativos, puede forjar tokens o llamadas API que Office 365 acepta como legítimas, ya que confía en el servidor interno.

- Las acciones del atacante no siempre generan logs detectables en Microsoft 365 (por ejemplo, Purview o registros de auditoría), lo que dificulta la detección

Explotación: No confirmada, pero considerada "muy probable" por Microsoft
Entornos afectados: Exchange Server 2016, 2019 y Subscription Edition con configuración híbrida activa.

Impacto potencial:

- Compromiso total del dominio híbrido, incluyendo buzones, calendarios y recursos compartidos.
- Acciones maliciosas en la nube que no quedan registradas o visibles mediante auditorías estándares.
- Alto riesgo en organizaciones con entornos híbridos que dependen de autenticaciones federadas.

Recomendaciones de mitigación:

- Aplicar de inmediato los *hotfixes* de abril 2025 para entornos Exchange híbridos, según guía oficial de Microsoft.
- Verificar y rehacer las KeyCredentials del Principal del Servicio, siguiendo el modo de limpieza recomendado por Microsoft.
- Ejecutar el verificador de salud de Microsoft Exchange (Health Checker) para identificar posibles brechas adicionales.
- Si ya no se usa Exchange híbrido, considerar desactivarlo o realizar migración a Exchange Online.
- Limitar el acceso administrativo al servidor On-Prem y auditarlos cuidadosamente en caso de compromisos previos.

Prioridad: Critica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/vulnerabilidad-permite-compromiso-total.html?utm_campaign=Segu-Info+-+Ciberseguridad+desde+el+2000&utm_content=Segu-Info+-+Ciberseguridad+desde+el+2000&utm_medium=SeguInfo&utm_source=SeguInfo
- https://www.techradar.com/pro/security/microsoft-urges-users-to-be-on-alert-following-high-severity-flaw-in-hybrid-exchange-deployments
- https://www.bleepingcomputer.com/news/security/over-29-000-exchange-servers-unpatched-against-high-severity-flaw/
- https://www.cisa.gov/news-events/directives/ed-25-02-mitigate-microsoft-exchange-vulnerability

PYPI PREVIENE ATAQUES DE PARSER CONFUSION EN ARCHIVOS WHEEL Y ZIP

PyPI publicó un aviso importante para mitigar un vector potencial donde archivos .whl malformados podían evadir instalaciones al tener discrepancias entre los encabezados ZIP y su archivo RECORD. Aunque no se han reportado explotaciones activas, la amenaza podría comprometer la cadena de suministro de Python

Resumen técnico:

- El problema se origina por ambigüedades heredadas del estándar ZIP: los instaladores pueden leer primero el directorio central o los encabezados locales.
- Un atacante podría manipular un archivo Wheel para que liste solo archivos benignos en RECORD, mientras que el archivo ZIP real contenga malware adicional bajo nombres distintos.
- PyPI detectó estas condiciones durante evaluaciones y decidió emitir una advertencia. Se implementarán validaciones estrictas en futuras cargas

Impacto potencial:

- Infección encubierta mediante la instalación de archivos maliciosos sin que el desarrollador se dé cuenta.

- Riesgo de backdoors o carga de código malicioso en entornos que consumen paquetes desde PyPI.
- Afectación severa a la confianza y seguridad en la cadena de suministro de desarrollo de software.

Acciones de prevención anunciadas

PyPI está rechazando archivos Wheel con archivos duplicados entre encabezados o datos RECORD inválidos. A partir del 1 de febrero de 2026, cualquier Wheel con discrepancia entre el contenido y su registro RECORD será bloqueado automáticamente tras un periodo de advertencia de seis meses.

Recomendaciones de mitigación:

- Actualizar herramientas de empaquetado e instalación (como pip, setuptools, wheel) para garantizar que usan lógicas de verificación compatibles.
- Rechazar manualmente o revisar Wheel con signos de inconsistencias en cabeceras ZIP o archivo RECORD.
- En entornos críticos, utilizar firmas o hashes verificados como parte del proceso de instalación.
- Escanear dependencias con soluciones SCA (como Snyk, etc.) y configurar alertas frente a paquetes malformados o habituales en supply chain attacks.
- Participar en auditorías de integridad del entorno Docker/pipeline para prevenir inserción de código oculto.

Prioridad: Urgente.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/08/aviso-de-pypi-para-prevenir-ataques-de.html
- https://www.varutra.com/ctp/threatpost/postDetails/PyPI-Blocks-Malicious-ZIP-Uploads-to-Prevent-Parser-Confusion-Attacks/OXNWekVDT3ZJNWh4SllveXY1c0JsUT09

- https://www.techradar.com/pro/security/python-devs-targeted-with-dangerous-phishing-attacks-heres-how-to-stay-safe

VULNERABILIDAD CRÍTICA ZERO-DAY EN WINRAR (CVE-2025-8088) EXPLOTADA EN ATAQUES REALES

Se ha descubierto una vulnerabilidad de traversal de rutas (path traversal) en WinRAR para Windows, identificada como CVE-2025-8088, que está siendo explotada activamente por grupos como *RomCom* y *Paper Werewolf*. La falla permite extraer archivos maliciosos en ubicaciones arbitrarias como las carpetas de inicio automático, posibilitando así una ejecución silenciosa de malware sin alertas visibles

Resumen técnico:

- CVE-2025-8088 permite que archivos comprimidos especialmente diseñados extraigan ejecutables en rutas como:
  - %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup (por usuario)
  - %ProgramData%\Microsoft\Windows\Start Menu\Programs\StartUp (todo el sistema)

- El exploit fue descubierto en campañas de spearphishing donde se adjuntaban archivos .RAR disfrazados de CVs. Al extraerlos, el malware se instala automáticamente para ejecutarse en el inicio.

- Grupos como *RomCom* (Storm-0978/UNC2596) han utilizado este exploit para desplegar backdoors como Mythic Agent, SnipBot y RustyClaw. Asimismo, *Paper Werewolf* ha exploitado la vulnerabilidad contra organizaciones rusas. La misma falla se ofreció en foros criminales por USD 80.000.

Impacto potencial:

- Compromiso persistente del sistema mediante ejecución automática de malware.
- Alta evasión de defensas, sin intervención del usuario tras extracción.

- Amenaza real a sectores críticos, incluyendo finanzas, manufactura, defensa y logística.
- Afecta a equipos sin parchear en todo el mundo, dada la popularidad de WinRAR.

Recomendaciones de mitigación:

- Actualizar manualmente WinRAR a la versión 7.13 o superior, que incluye la corrección.
- Esta versión corrige tanto CVE-2025-8088 como un fallo anterior (CVE-2025-6218), parcheado en la 7.12.
- Auditar el sistema por archivos RAR sospechosos que contengan payloads ADS ocultos o enlaces a carpetas de inicio.
- Implementar detección en EDR / SIEM, utilizando reglas como las sugeridas por SOC Prime para CVE-2025-8088.
- Educar a usuarios para desconfiar de archivos RAR enviados como CVs u otros documentos de phishing.

Prioridad: Critica.

Ampliar Información:

- https://www.welivesecurity.com/es/seguridad-digital/winrar-corrige-vulnerabilidad-permite-comprimidos-ejecutar-malware/
- https://www.wiz.io/vulnerability-database/cve/cve-2025-6218
- https://nvd.nist.gov/vuln/detail/CVE-2025-8088
- https://www.scworld.com/news/winrar-zero-day-exploited-by-romcom-threat-group
- https://arstechnica.com/security/2025/08/high-severity-winrar-0-day-exploited-for-weeks-by-2-groups/
- https://www.bleepingcomputer.com/news/security/winrar-zero-day-flaw-exploited-by-romcom-hackers-in-phishing-attacks/
- https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

REVAULT — FALLA DE FIRMWARE CRÍTICA EN DELL CONTROLVAULT3 QUE PERMITE PERSISTENCIA PROFUNDA Y BYPASS DE AUTENTICACIÓN

Cisco Talos ha descubierto cinco vulnerabilidades críticas en el firmware ControlVault3 y sus APIs de Windows, conocido como ataque ReVault. Aunque diseñadas para proteger credenciales mediante un enclave seguro (USH), estas fallas permiten comprometer de forma persistente máquinas Dell sin que se detecte

Resumen técnico:
Se identificaron cinco fallas graves:

- *Out-of-bounds read/write* (CVE-2025-24311, CVE-2025-25050)
- *Arbitrary free* (CVE-2025-25215)
- *Stack-based buffer overflow* (CVE-2025-24922)
- *Unsafe deserialization* (CVE-2025-24919)

  Estas vulnerabilidades permiten ejecutar código arbitrario en el firmware.

Persistencia extrema: El malware implantado a nivel de firmware sobrevive reinstalaciones completas de sistema operativo, convirtiéndose en amenaza oculta.
Bypass de autenticación: Con acceso físico, se puede modificar el firmware para que acepte cualquier huella dactilar o credenciales, anulando mecanismos de login y cifrado.
No se necesita contraseña ni acceso previo al sistema
Alcance: Más de 100 modelos Dell Latitude y Precision, usados ampliamente en sectores sensibles como gobierno, industria y seguridad.

Impacto potencial:

- Persistencia invisible: Bajo el radar de antivirus, puede reconectar el malware tras reinstalaciones del sistema operativo.
- Control físico total: Quien acceda al hardware físico con un conector USB especial puede comprometer completamente la máquina.
- Alto riesgo en ambientes corporativos y gubernamentales: Dell es ampliamente utilizado en entornos de alta seguridad, por lo que las consecuencias pueden ser devastadoras

Recomendaciones de mitigación:

- Actualizar firmware y drivers de ControlVault3 a la versión más reciente disponible desde Windows Update o el sitio de soporte Dell.
- Deshabilitar dispositivos no esenciales como lectores biométricos, smartcards o NFC si no son necesarios.
- Habilitar detección de intrusión física (chassis intrusion) en BIOS y activar las opciones de seguridad avanzada en Windows (ESS).
- Monitorear actividad anómala del sistema relacionada con ControlVault y logs de autenticación.
- Evaluar seguridad de dispositivos críticamente en riesgo y considerar reemplazo si no se pueden parchear.

Prioridad: Critica.

Ampliar Información:

- https://www.helpnetsecurity.com/2025/08/05/dell-laptops-firmware-vulnerabilities-revault-attacks/
- https://www.securityweek.com/flaws-expose-100-dell-laptop-models-to-implants-windows-login-bypass/
- https://www.darkreading.com/vulnerabilities-threats/revault-security-flaws-dell-laptops
- https://www.bleepingcomputer.com/news/security/revault-flaws-let-hackers-bypass-windows-login-on-dell-laptops/
- https://blog.talosintelligence.com/revault-when-your-soc-turns-against-you/

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 Serve

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

CAPTCHAGEDDON — CAMPAÑA DE MALWARE QUE EXPLOTA CAPTCHAS FALSOS PARA EJECUCIÓN REMOTA (CLICKFIX)

Investigadores de seguridad han identificado una sofisticada campaña llamada CaptchaGeddon, también conocida como *ClickFix*, que reemplaza los típicos esquemas de falsos "browser updates" con CAPTCHAs falsos que engañan a los usuarios para que ejecuten comandos maliciosos. Medios técnicos como The Hacker News y Cybersecurity News usan el término para destacar su rápida expansión y efectividad

Resumen técnico:

- La víctima visita una página con un CAPTCHA falso, que simula verificaciones legítimas como reCAPTCHA o similares.
- Al pulsar "Verify", el sitio copia un comando peligroso al portapapeles y guía al usuario para que lo pegue (Ctrl+V) en el cuadro "Ejecutar" de Windows o en la Terminal.
- Al ejecutarlo, se lanzan scripts que descargan y ejecutan malware como stealer (p. ej. Lumma Stealer), troyanos de acceso remoto (RATs) o loaders.
- La campaña ha alcanzado ambientes Windows, macOS y Linux, eliminando la necesidad de descargas visibles y evitando detecciones automatizadas.

- Propagación efectiva vía malvertising, sitios comprometidos (WordPress), SEO malicioso y phishing

Impacto potencial:

- Alto alcance de infección por su carácter multiplataforma y uso de infraestructura confiable (p. ej. Google Scripts, dominios legítimos).
- Riesgo elevado por su eficacia en usuarios desprevenidos: viola la confianza al disfrazarse de protección.
- Compromiso efectivo de credenciales sensibles, sesiones activas y dispositivos personales o corporativos.
- Se observa una adopción amplia y rápida entre atacantes, desplazando campañas anteriores como los falsos updates de navegador

Recomendaciones de mitigación:

- Educar a los usuarios: advertir que los CAPTCHAs no legítimos nunca requieren copiar y ejecutar comandos.
- Bloquear scripts sospechosos: uso de control de ejecución (AppLocker, PowerShell firmado) para impedir ejecución de comandos no autorizados.
- Monitorear comportamiento atípico: detectar actividad de portapapeles, ejecuciones automáticas de línea de comandos y descargas desde dominios sospechosos.
- Filtrar contenido web y DNS: bloquear dominios asociados, malvertising y CAPTCHA falsos con sistemas de prevención web.
- Ejecutar simulacros de phishing que incluyan este vector para reforzar concienciación de empleados.

Prioridad: Urgente.

Ampliar Información:

- https://arcticwolf.com/resources/blog/widespread-fake-captcha-campaign-delivering-malware/

- https://guard.io/labs/captchageddon-unmasking-the-viral-evolution-of-the-clickfix-browser-based-threat
- https://cybersecuritynews.com/captchageddon-new-clickfix-attack/
- https://thehackernews.com/2025/08/clickfix-malware-campaign-exploits.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

GOOGLE Y OTRAS EMPRESAS SUFREN ROBO DE DATOS VÍA SALESFORCE POR EL GRUPO SHINYHUNTERS

Una campaña de robo de información ha comprometido instancias de Salesforce CRM usadas por *Google* y diversas organizaciones, perpetrada por el grupo extorsionista ShinyHunters. Se trata de una oleada de intrusiones enfocadas en capturar datos sensibles desde plataformas de CRM

.

Resumen técnico

- Google confirmó que ShinyHunters accedió a su instancia de Salesforce, extrayendo información interna relacionada con clientes, incluyendo detalles de contacto y notas de soporte. No se divulgaron contraseñas ni información financiera.
- El ataque afecta a múltiples empresas globales que utilizan Salesforce para gestión de relaciones con clientes.
- Google ya había alertado sobre intentos previos de robo mediante ingeniería social destinados a plataformas Salesforce corporativas.

Impacto potencial

- Exposición de información de clientes y empresas, lo que puede derivar en ingeniería social, phishing personalizado (spear-phishing) o extorsión.
- Pérdida de confianza por parte de clientes impactados y exposición reputacional, especialmente para marcas globales como Google.
- Riesgo elevado de movimientos laterales o explotación adicional si se obtienen credenciales administrativas o acceso persistente en Salesforce.

Recomendaciones para mitigar el riesgo:

- Reforzar seguridad en Salesforce:
  - Habilitar autenticación fuerte (MFA con FIDO2 o similares).
  - Implementar monitoreo continuo de actividades anómalas dentro de la plataforma.
- Auditar accesos y sesiones en Salesforce, revisando historiales de acceso y exportación masiva de datos.
- Capacitar a usuarios comerciales y de soporte para reconocer intentos de phishing o ingeniería social dirigidos a funcionalidades CRM.
- Reforzar políticas de acceso a Salesforce, incluyendo segmentación de privilegios por rol y revisiones periódicas de permisos.

- Mitigar exfiltraciones futuras, implementando herramientas DLP que supervisen exportaciones inusuales desde plataformas CRM.

Prioridad: Importante.

Ampliar Información:

- https://www.crn.com/news/security/2025/5-things-to-know-on-salesforce-data-theft-attacks
- https://blog.segu-info.com.ar/2025/08/salesforce-google-y-otras-empresas.html
- https://www.bleepingcomputer.com/news/security/google-hackers-target-salesforce-accounts-in-data-extortion-attacks
- https://eye.world/cyber%E2%80%91threat-alert-hits-google-via-salesforce-breach/