GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2025

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

VULNERABILIDADES

ANÁLISIS: NUEVAS VULNERABILIDADES EN CPUS INTEL REAVIVAN EL FANTASMA DE SPECTRE V2

Investigadores de la ETH Zürich y la Vrije Universiteit Amsterdam han identificado dos nuevas vulnerabilidades que afectan a prácticamente todos los procesadores Intel modernos. Estas fallas permiten la lectura de memoria ajena incluso cuando están activadas las mitigaciones contra Spectre implementadas desde 2018.

Branch Privilege Injection (BPI): Esta vulnerabilidad explota condiciones de carrera en el predictor de saltos durante transiciones de privilegios, permitiendo que un proceso no privilegiado inyecte predicciones que serán utilizadas por procesos con mayores privilegios. Esto puede resultar en la filtración de memoria a una velocidad de aproximadamente 5,6 KiB/s.

Training Solo: Esta técnica permite a un atacante "entrenar" al predictor de saltos utilizando únicamente código existente dentro del propio kernel o hipervisor, eludiendo las barreras de aislamiento de dominio. Las vulnerabilidades asociadas son:

- CVE-2024-28956: Indirect Target Selection (ITS)
- CVE-2025-24495: Fallo en el núcleo Lion Cove
  Estas fallas permiten velocidades de filtración de hasta 17 KB/s

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2024-45332: Branch Privilege Injection (BPI)
- CVE-2024-28956: Indirect Target Selection (ITS)
- CVE-2025-24495: Fallo en el núcleo Lion Cove

Recomendaciones de mitigación:

- Aplicar actualizaciones de firmware y sistema operativo: Implementar las actualizaciones proporcionadas por Intel y los fabricantes de sistemas operativos tan pronto como estén disponibles.
- Monitorear entornos compartidos: En entornos multi-inquilino, considerar la implementación de medidas adicionales de aislamiento y monitoreo para detectar posibles actividades maliciosas.
- Evaluar el impacto en el rendimiento: Algunas mitigaciones pueden tener un impacto en el rendimiento del sistema; es importante evaluar y planificar en consecuencia.

Prioridad: Critica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/05/nuevas-vias-de-fuga-de-memoria-en-cpus-intel-reavivan-el-fantasma-de-spectre-v2.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01247.html

- https://www.linkedin.com/pulse/new-intel-cpu-vulnerabilities-allows-memory-leaks-cajne
- https://thehackernews.com/2025/05/researchers-expose-new-intel-cpu-flaws.html
- https://www.it-experience.cl/nuevos-hallazgos-de-fuga-de-memoria-en-procesadores-intel/

ANÁLISIS: VULNERABILIDAD 0-DAY EN GOOGLE CHROME (CVE-2025-4664)

Una vulnerabilidad crítica de tipo 0-day, identificada como CVE-2025-4664, ha sido descubierta en el navegador Google Chrome. Esta falla permite a atacantes remotos filtrar datos de origen cruzado mediante una página HTML especialmente diseñada, incluso en versiones actualizadas del navegador

Resumen técnico:

- Descripción de la vulnerabilidad: La falla reside en el componente Loader de Chrome, responsable de manejar las solicitudes de recursos. Debido a una aplicación insuficiente de políticas de seguridad, un atacante puede explotar la cabecera Link para establecer una política de referencia (referrer-policy) que incluya URL completas, permitiendo la filtración de parámetros sensibles
- Impacto potencial: La explotación exitosa de esta vulnerabilidad podría permitir a un atacante acceder a información confidencial, como tokens de autenticación o credenciales, facilitando el secuestro de cuentas y otras actividades maliciosas.
- Explotación activa: Google ha confirmado que existe un exploit para esta vulnerabilidad en circulación. Además, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incluido CVE-2025-4664 en su catálogo de vulnerabilidades explotadas activamente, exigiendo a las agencias federales aplicar las correcciones antes del 5 de junio de 2025

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-4664: Insuficiente aplicación de políticas en el componente Loader de Google Chrome.

Impacto y mitigaciones:

Sistemas afectados: Todas las versiones de Google Chrome anteriores a la 136.0.7103.113 en Windows y Linux, y 136.0.7103.114 en macOS.

Mitigación: Actualizar Google Chrome a las versiones mencionadas. Para verificar y aplicar la actualización:

- Abrir Chrome.
- Ir a Configuración > Información de Chrome.
- El navegador buscará actualizaciones automáticamente y solicitará reiniciar para completar el proceso.

Otros navegadores afectados: Navegadores basados en Chromium, como Microsoft Edge, Brave, Opera y Vivaldi, también podrían verse afectados y deben aplicar las actualizaciones correspondientes cuando estén disponibles.

Recomendaciones de mitigación:

- Actualizar el navegador: Aplicar inmediatamente las actualizaciones de seguridad proporcionadas por Google para mitigar la vulnerabilidad.
- Revisar configuraciones de seguridad: Asegurarse de que las políticas de seguridad del navegador estén correctamente configuradas para minimizar riesgos.
- Monitorear actividad sospechosa: Estar atento a comportamientos inusuales en cuentas y sistemas que puedan indicar explotación de la vulnerabilidad.

Prioridad: Critica.

Ampliar Información:

- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidad-0-day-en-google-chrome/webcyb00-contcibglos/es/
- https://thehackernews.com/2025/05/new-chrome-vulnerability-enables-cross.html
- https://www.malwarebytes.com/blog/news/2025/05/update-your-chrome-to-fix-serious-actively-exploited-vulnerability
- https://threatprotect.qualys.com/2025/05/15/google-releases-fix-for-zero-day-vulnerability-in-chrome-cve-2025-4664/
- https://thehackernews.com/2025/05/new-chrome-vulnerability-enables-cross.html

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

Alerta: instaladores falsos de rvtools propagan malware de robo de información

La reconocida herramienta RVTools, ampliamente utilizada para la administración de entornos VMware, ha sido objeto de una campaña maliciosa en la que ciberdelincuentes distribuyen instaladores falsos que contienen malware diseñado para robar

Resumen técnico:

- Distribución del malware: Los atacantes crean sitios web que imitan al oficial de RVTools, ofreciendo descargas de instaladores maliciosos. Estos sitios fraudulentos se posicionan en los resultados de búsqueda mediante técnicas de SEO y anuncios patrocinados.
- Método de infección: El instalador falso, generalmente empaquetado en archivos ZIP, instala junto a la herramienta legítima un malware que opera de forma silenciosa.
- Funcionalidad del malware: Una vez ejecutado, el malware recopila y exfiltra información como credenciales, datos de navegadores, carteras de criptomonedas y otros archivos sensibles.
-

Recomendaciones para mitigar el riesgo:

- Descargar desde fuentes oficiales: Asegurarse de obtener RVTools únicamente desde su sitio web oficial y evitar enlaces de terceros.
- Verificar la integridad de los archivos: Comparar las sumas de verificación (hash) proporcionadas por el desarrollador para confirmar la autenticidad del instalador.
- Mantener el software actualizado: Tanto el sistema operativo como las herramientas de seguridad deben estar al día para detectar y prevenir amenazas.
- Cautela con resultados patrocinados: Evitar hacer clic en anuncios patrocinados que puedan redirigir a sitios maliciosos.

Prioridad: Urgente.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/05/rvtools-instalar-la-popular-herramienta-ahora-puede-infectar-tu-sistema.html

Análisis: más de 100 extensiones falsas de Chrome detectadas robando credenciales y secuestrando sesiones

Una campaña maliciosa activa desde febrero de 2024 ha distribuido más de 100 extensiones de Chrome falsas, diseñadas para robar credenciales, secuestrar sesiones, inyectar anuncios y ejecutar código arbitrario. Estas extensiones, que aparentan ser herramientas legítimas como VPNs, asistentes de IA y utilidades de productividad, han sido eliminadas por Google, pero muchas permanecieron activas durante meses en la Chrome Web Store.

Resumen técnico:R

- Mecanismo de infección: Las extensiones se promocionaban a través de sitios web falsos que imitaban servicios legítimos como DeepSeek, FortiVPN y DeBank. Una vez instaladas, solicitaban permisos excesivos mediante el archivo manifest.json, permitiéndoles interactuar con todos los sitios visitados, ejecutar código desde dominios controlados por atacantes y establecer conexiones WebSocket para redirigir tráfico.
- Técnicas de evasión: Utilizaban el evento onreset en elementos DOM temporales para ejecutar código, posiblemente para evadir políticas de seguridad de contenido (CSP). Además, manipulaban las calificaciones en la Chrome Web Store, redirigiendo a los usuarios que dejaban reseñas negativas a formularios privados, mientras que las reseñas positivas se publicaban normalmente.
- Impacto: Estas extensiones permitían a los atacantes robar cookies de sesión, credenciales y tokens de autenticación, facilitando el secuestro de cuentas y la ejecución de campañas de phishing.

Recomendaciones para mitigar el riesgo:

- Auditar extensiones instaladas: Revisar y eliminar cualquier extensión no reconocida o sospechosa.
- Verificar permisos: Evitar extensiones que soliciten permisos innecesarios o excesivos.
- Instalar desde fuentes confiables: Preferir extensiones de desarrolladores verificados y con buena reputación.
- Monitorear comportamiento del navegador: Estar atento a comportamientos inusuales, como redirecciones inesperadas o aparición de anuncios no solicitados.

Prioridad: Critica.

Ampliar Información:

- https://thehackernews.com/2025/05/100-fake-chrome-extensions-found.html
- https://time.com/3850461/browser-ad-injectors

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

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

Análisis: la actualización KB5058379 provoca la pantalla de recuperación Bitlocker en algunos equipos con Windows 10

La actualización acumulativa KB5058379, lanzada por Microsoft el 13 de mayo de 2025 como parte del Patch Tuesday, ha generado problemas en ciertos dispositivos con Windows 10. Tras su instalación, algunos sistemas arrancan directamente en el Entorno de Recuperación de Windows (WinRE), solicitando la clave de recuperación de BitLocker, incluso sin cambios aparentes en la configuración del sistema.

- Causa del problema: La actualización KB5058379 introduce modificaciones en módulos relacionados con el arranque seguro y la medición de integridad del sistema. En equipos con procesadores Intel de 10ª generación o superiores que tienen habilitada la tecnología Intel Trusted Execution Technology (TXT), estas modificaciones pueden alterar los valores que el TPM (Trusted Platform Module) verifica durante el arranque. Si la verificación no coincide, BitLocker interpreta que el disco pudo haber sido manipulado y exige la clave de recuperación
- Dispositivos afectados: Se han reportado casos en equipos de marcas como Lenovo, Dell y HP. Los sistemas más propensos a este problema son aquellos con Windows 10 22H2, Windows 10 Enterprise LTSC 2021 y Windows 10 IoT Enterprise LTSC 2021, especialmente si utilizan procesadores Intel vPro con TXT habilitado
- Solución provisional: Microsoft ha lanzado la actualización de emergencia KB5061768 para abordar este problema. Esta actualización está disponible a través del Microsoft Update Catalog y se recomienda su instalación en los sistemas afectados.

Recomendaciones para organizaciones:

- Instalar la actualización KB5061768: Aplicar esta actualización de emergencia en los sistemas afectados para resolver el problema de la pantalla de recuperación de BitLocker.

- Verificar la configuración del BIOS/UEFI: Si la actualización no está disponible o no resuelve el problema, considerar deshabilitar temporalmente Intel TXT, Secure Boot y las funciones de virtualización (VT-x/VT-d) en la configuración del BIOS/UEFI. Sin embargo, estas acciones pueden reducir la seguridad del sistema y deben realizarse con precaución
- Custodiar la clave de recuperación de BitLocker: Asegurarse de tener acceso a la clave de recuperación de BitLocker antes de aplicar actualizaciones que puedan afectar el arranque del sistema.

Prioridad: Importante.

Ampliar Información:

- https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5058379-update-triggering-bitlocker-recovery-after-install/
- https://support.microsoft.com/en-us/topic/may-13-2025-kb5058379-os-builds-19044-5854-and-19045-5854-0a30e9ee-5038-45dd-a5d7-70a8813a5e39
- https://unaaldia.hispasec.com/2025/05/la-actualizacion-kb5058379-provoca-la-pantalla-de-recuperacion-bitlocker-en-algunos-equipos-con-windows-10.html
- https://www.techzine.eu/news/security/131572/windows-10-emergency-update-resolves-bitlocker-startup-issues/
- https://www.bleepingcomputer.com/news/microsoft/windows-10-emergency-updates-fix-bitlocker-recovery-issues/
- https://www.laptopmag.com/laptops/windows-laptops/windows-update-bitlocker-bug

Análisis: Google Chrome ahora puede cambiar automáticamente contraseñas comprometidas usando su gestor integrado

Google ha anunciado una nueva función en su navegador Chrome que permite al Gestor de Contraseñas integrado cambiar automáticamente las contraseñas de los usuarios

cuando detecta que han sido comprometidas. Esta característica busca simplificar la gestión de contraseñas y mejorar la seguridad del usuario al automatizar el proceso de actualización de credenciales en sitios web compatibles

Resumen técnico:

- Detección de contraseñas comprometidas: Cuando Chrome detecta que una contraseña ha sido comprometida durante el inicio de sesión, el Gestor de Contraseñas de Google alerta al usuario y ofrece la opción de corregirla automáticamente
- Generación y actualización automática: En sitios web compatibles, Chrome puede generar una contraseña segura y reemplazar la comprometida sin intervención manual del usuario
- Requisitos para desarrolladores web: Para que esta función esté disponible, los desarrolladores deben implementar ciertos estándares, como el uso de los atributos autocomplete="current-password" y autocomplete="new-password", y configurar una redirección desde /.well-known/change-password al formulario de cambio de contraseña del sitio
- Consentimiento del usuario: Aunque el proceso es automatizado, Chrome siempre solicitará el consentimiento del usuario antes de realizar cualquier cambio en las contraseñas

Recomendaciones para organizaciones:

- Mantener Chrome actualizado: Asegúrese de utilizar la última versión de Chrome para acceder a esta y otras funciones de seguridad mejoradas.
- Revisar las contraseñas almacenadas: Utilice el Gestor de Contraseñas de Google para identificar y actualizar contraseñas débiles o comprometidas.
- Implementar buenas prácticas de seguridad: Considere el uso de autenticación de dos factores (2FA) y evite reutilizar contraseñas en múltiples sitios.

Prioridad: Importante.

Ampliar Información:

- https://www.theverge.com/news/670208/google-chrome-passwords-auto-update-io-2025
- https://thehackernews.com/2025/05/google-chrome-can-now-auto-change.html