GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2125

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	1
MALWARE	0	0	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

Vulnerabilidad crítica en Google Chrome (CVE-2025-4664)

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

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.

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

y la política de referencia (referrer-policy) para forzar el envío de datos sensibles, como tokens de autenticación o credenciales temporales, a destinos no seguros.

- 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: La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incluido CVE-2025-4664 en su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), confirmando que existe un exploit para esta vulnerabilidad en circulación.

Los CVE relacionados a este compromiso de seguridad son:

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

Recomendaciones de 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.

Nota: 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.

Prioridad: Critica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/05/chrome-bajo-ataque-vulnerabilidad-critica-cve-2025-4664.html

Vulnerabilidad crítica en Bitwarden permite ejecución de Javascript malicioso desde archivos pdf (cve-2025-5138)

Una vulnerabilidad de tipo cross-site scripting (XSS), identificada como CVE-2025-5138, ha sido descubierta en Bitwarden, afectando a versiones hasta la 2.25.1. Esta falla permite a atacantes con cuentas de bajo privilegio subir archivos PDF manipulados que, al ser visualizados por otros usuarios, ejecutan código JavaScript malicioso en el contexto de la aplicación

- Componente afectado: PDF File Handler utilizado por la función "Resources" de Bitwarden.
- Vector de ataque: Un atacante con una cuenta (aunque sea de bajo privilegio) puede subir un archivo PDF especialmente diseñado que contiene JavaScript malicioso. Cuando otro usuario visualiza este PDF dentro de la plataforma, el código se ejecuta en su navegador.
- Impacto potencial: Robo de tokens de sesión, ejecución de acciones en nombre del usuario y posible acceso no autorizado a la bóveda de contraseñas.
- Prueba de concepto: El investigador YZS17 ha publicado un proof-of-concept en GitHub demostrando la explotación de esta vulnerabilidad

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-5138: Vulnerabilidad de tipo XSS en el manejador de archivos PDF de Bitwarden

Recomendaciones de mitigación:

- Actualizar Bitwarden: Estar atento a las actualizaciones oficiales y aplicar los parches de seguridad tan pronto como estén disponibles.

- Capacitación del personal: Informar a los usuarios sobre los riesgos asociados con la apertura de archivos PDF dentro de la plataforma y fomentar prácticas seguras.
- Monitoreo de actividad sospechosa: Vigilar posibles accesos no autorizados o actividades inusuales en las cuentas de los usuarios.

Prioridad: Importante.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/05/bitwarden-expone-a-sus-usuarios-a-javascript-malicioso-incrustado-en-pdfs.html
- https://cybersecuritynews.com/bitwarden-pdf-file-handler-vulnerability/
- https://gbhackers.com/bitwarden-flaw/

VMware corrige múltiples vulnerabilidades de alta gravedad

VMware ha abordado recientemente varias vulnerabilidades críticas que afectan a sus productos, incluyendo ESXi, Workstation, Fusion, Cloud Foundation, Aria Operations y Avi Load Balancer. Algunas de estas fallas están siendo explotadas activamente, lo que subraya la urgencia de aplicar las actualizaciones correspondientes

Productos afectados y versiones:

- VMware ESXi: Versiones 7.0 y 8.0.
- VMware Workstation: Versiones 17.x.
- VMware Fusion: Versiones 13.x.
- VMware Cloud Foundation: Versiones 4.x y 5.x.
- VMware Aria Operations: Versiones 8.x.
- VMware Avi Load Balancer: Versiones 30.1.1, 30.1.2, 30.2.1 y 30.2.2

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-22224
- CVE-2025-22225
- CVE-2025-22226
- CVE-2025-22230
- CVE-2025-22217

Prioridad: Critica.

Ampliar Información:

- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2025-22230
- https://unaaldia.hispasec.com/2025/03/tres-vulnerabilidades-activas-en-vmware-actualizacion-obligatoria.html
- https://ostec.blog/es/generico/cve-2025-22217-vulnerabilidad-de-inyeccion-de-sql-en-vmware-avi-load-balancer/
- https://www.cert.gov.py/vulnerabilidades-en-productos-vmware-3/

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

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

Integraciones con OneDrive File Picker exponen archivos completos por mala gestión de permisos

Investigadores de OASIS Security revelaron que múltiples aplicaciones que utilizan la herramienta Microsoft OneDrive File Picker pueden acceder a la totalidad del almacenamiento del usuario en OneDrive, incluso cuando el usuario solo selecciona un archivo para compartir. Esto se debe a permisos excesivos solicitados mediante OAuth y a mensajes de consentimiento confusos, lo que puede derivar en acceso no intencionado a todos los archivos.

Resumen técnico:

- Permisos excesivos: Al integrar el Picker, las apps solicitan Files.Read, que concede acceso completo, incluso si solo se va a subir o seleccionar un archivo.
- Mensajes de consentimiento ambiguos: El usuario acepta sin saber que otorga acceso total.
- Tokens almacenados de forma insegura: Algunos servicios almacenan access_token y refresh_token en el sessionStorage del navegador, lo que facilita su robo en caso de XSS.
- Servicios afectados: ChatGPT, Slack, ClickUp, Trello, entre otros.

Recomendaciones para mitigar el riesgo:

Para Usuarios:

- Revisar y revocar accesos desde: https://account.live.com/consent/Manage
- Evitar subir información sensible a través de integraciones que usen OneDrive File Picker.
- Activar autenticación multifactor (MFA) en cuentas Microsoft.

Para desarrolladores:

- Evitar Files.Read y offline_access si no son necesarios.
- Implementar OAuth con scopes mínimos requeridos.
- Almacenar tokens de forma segura, evitando sessionStorage.
- Utilizar /.well-known/change-password y buenas prácticas de consentimiento claro.

Prioridad: Importante

Ampliar Información:

- https://thehackernews.com/2025/05/microsoft-onedrive-file-picker-flaw.html
- https://www.oasis.security/resources/blog/onedrive-file-picker-security-flaw-oasis-research