GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °5125

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	0	1

VULNERABILIDADES

GOOGLE CHROME — VULNERABILIDAD ZERO-DAY DE ALTA SEVERIDAD EXPLOTADA ACTIVAMENTE (ISSUE 466192044)

Google ha publicado una actualización de seguridad de emergencia para el navegador Chrome con el fin de corregir una vulnerabilidad zero-day de alta severidad que está siendo explotada activamente en entornos reales. La falla, identificada internamente como Issue 466192044, se mantiene bajo divulgación restringida mientras el proveedor acelera el despliegue del parche y los equipos de seguridad priorizan su aplicación.

El parche fue liberado a través del canal estable, elevando Chrome a la versión 143.0.7499.109/.110 para Windows y macOS, y 143.0.7499.109 para Linux. La actualización también corrige dos vulnerabilidades adicionales de severidad media reportadas por investigadores externos.

Resumen técnico:

- Identificador principal: Issue 466192044 (Zero-day, explotada activamente – detalles técnicos no divulgados).
- Estado: Explotación activa confirmada ("Under coordination").
- CVE-2025-14372 (Severidad Media): Vulnerabilidad de tipo use-after-free en el Gestor de Contraseñas, que podría derivar en corrupción de memoria o ejecución arbitraria de código.
- CVE-2025-14373 (Severidad Media): Implementación inapropiada en la barra de herramientas del navegador.
- Versiones afectadas:
- Google Chrome versiones anteriores a 143.0.7499.109/.110 (Windows y macOS).
- Google Chrome versiones anteriores a 143.0.7499.109 (Linux).

Impacto potencial:

- Compromiso del navegador mediante explotación remota sin parche previo.
- Posible ejecución de código arbitrario en el contexto del proceso del navegador.
- Riesgo elevado en entornos corporativos donde Chrome es el navegador estándar, especialmente en puestos de alto valor o con acceso a información sensible.
- Exposición previa potencial en sistemas que no hayan aplicado la actualización antes del despliegue del parche.

Recomendaciones de mitigación:

1. Actualización inmediata: Priorizar la actualización de Google Chrome a la versión 143.0.7499.109/.110 (Windows y macOS) o 143.0.7499.109 (Linux).
2. Reinicio del navegador: Asegurar el reinicio de Chrome tras la actualización para que el parche se aplique correctamente.
3. Gestión corporativa: Forzar actualizaciones automáticas del navegador en entornos empresariales mediante políticas de gestión centralizada.
4. Monitoreo post-parcheo: Revisar telemetría de EDR, proxy y firewall en busca de posibles intentos de explotación previos a la actualización.

Prioridad: Crítica.

Ampliar información:

- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-zero-day-en-google-chrome-2/
- https://socprime.com/es/blog/cve-2025-62221-and-cve-2025-54100-vulnerabilities/
- https://unaaldia.hispasec.com/2025/12/google-parchea-una-nueva-0-day-critica-en-chrome-en-plena-campana-de-explotacion.html
- https://computerhoy.20minutos.es/ciberseguridad/actualiza-ya-google-arregla-su-octavo-zero-day-chrome-2025-tras-nuevos-ataques_6909551_0.html

MICROSOFT WINDOWS — INCREMENTO DE ZERO-DAYS Y NUEVO FALLO NO PARCHEADO EN RASMAN

Durante 2025, Microsoft ha corregido más de 1.100 vulnerabilidades a través de sus ciclos de actualización Patch Tuesday, entre las cuales se incluyen al menos 41 vulnerabilidades zero-day. De estas, 24 fueron explotadas activamente en entornos reales al momento de su divulgación. Investigaciones recientes han puesto de relieve que, pese a los parches publicados, continúan apareciendo nuevos zero-days asociados a componentes críticos de Windows, como el servicio Remote Access Connection Manager (RasMan).

En este contexto, investigadores de ACROS Security identificaron una nueva vulnerabilidad zero-day de denegación de servicio en RasMan, descubierta durante el análisis de la CVE-2025-59230, lo que reabre escenarios de ataque que se consideraban mitigados tras los parches de octubre.

Resumen técnico:

- Sin CVE asignado (relacionado con CVE-2025-59230)
- Vector de ataque: Local
- Causa raíz: Manejo incorrecto de listas enlazadas circulares en el servicio RasMan.
- Estado: No parcheado oficialmente por Microsoft al momento del reporte.
- Condición de explotación: Ejecución de código local sin privilegios y provocación intencional del fallo del servicio RasMan.
- Impacto técnico: Denegación de servicio del componente RasMan y posible encadenamiento con CVE-2025-59230 para elevación de privilegios.
- Versiones afectadas: Windows 7 a Windows 11 y Windows Server 2008 R2 a Windows Server 2025.
- Plataformas impactadas: Sistemas Windows cliente y servidor con RasMan habilitado.

Impacto potencial:

- Interrupción de servicios de acceso remoto (VPN, PPPoE).
- Incremento del riesgo de escalamiento de privilegios en sistemas locales.
- Exposición prolongada ante ausencia de parche oficial.

Recomendaciones de mitigación:

1. Aplicar los parches oficiales de Microsoft relacionados con CVE-2025-59230.
2. Evaluar la instalación del microparche gratuito de ACROS Security (0patch).
3. Monitorear eventos asociados a fallos del servicio RasMan.
4. Revisar políticas de privilegios locales y controles de acceso.

Prioridad: Urgente.

Ampliar información:

- https://www.theregister.com/2025/12/12/microsoft_windows_rasman_dos_0day/
- https://www.softzone.es/noticias/windows/google-revelaar-vulnerabilidad-windows-11-enfurecer/
- https://www.securitylab.lat/news/567175.php
- https://blog.segu-info.com.ar/2025/12/microparche-para-nuevo-zero-day-en.html
- https://www.forbes.com/sites/daveywinder/2025/12/14/41-microsoft-zero-days---now-millions-of-users-face-update-choice/

REACT SERVER COMPONENTS — FALLOS EN RSC PERMITEN DoS Y EXPOSICIÓN DE CÓDIGO FUENTE

El equipo de React publicó correcciones de seguridad para React Server Components (RSC) tras identificarse nuevas vulnerabilidades durante el análisis de parches previos asociados a React2Shell (CVE-2025-55182). Los fallos permiten provocar denegación de servicio sin autenticación y, bajo ciertas condiciones, exponer el código fuente de funciones del servidor.

Resumen técnico:

- Identificadores principales:
- CVE-2025-55184 (CVSS 7.5): Denegación de servicio por deserialización insegura de solicitudes HTTP en React Server Functions, provocando bloqueo del proceso del servidor.
- CVE-2025-67779 (CVSS 7.5): Corrección incompleta de CVE-2025-55184 que permite nuevamente la denegación de servicio mediante payloads especialmente diseñados.
- CVE-2025-55183 (CVSS 5.3): Exposición de información que puede devolver el código fuente de funciones del servidor a través de solicitudes HTTP manipuladas.

- Vector de ataque: Remoto, vía solicitudes HTTP a Server Functions / Server Actions
- Tipo de vulnerabilidad: Denegación de Servicio (DoS) y exposición de información (código fuente)
- Causa raíz: Deserialización insegura de payloads HTTP en endpoints de Server Functions y corrección incompleta de parches previos (bypass)
- Condición de explotación: No requiere autenticación, payload HTTP especialmente diseñado y para CVE-2025-55183, existencia de Server Functions que expongan argumentos convertidos a string
- Versiones afectadas:
- react-server-dom-parcel
- react-server-dom-turbopack
- react-server-dom-webpack

Impacto potencial:

- Indisponibilidad del servicio en aplicaciones React en producción.
- Exposición de lógica interna del servidor.
- Incremento del riesgo si existen secretos embebidos en el código.
- Escenarios de explotación masiva dada la amplia adopción de React.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a versiones corregidas: 19.0.3, 19.1.4 y 19.2.3
2. Revisar el uso de Server Functions expuestas públicamente
3. Monitorear patrones anómalos de solicitudes HTTP hacia endpoints RSC
4. Priorizar el parcheo debido a actividad previa de explotación en el ecosistema React

Prioridad: Urgente.

Ampliar información:

- https://unit42.paloaltonetworks.com/es-la/cve-2025-55182-react-and-cve-2025-66478-next/
- https://unaaldia.hispasec.com/2025/12/react-corrige-nuevos-fallos-en-rsc-que-provocan-dos-y-exponen-codigo-fuente.html
- https://socprime.com/es/blog/cve-2025-14174-vulnerability/
- https://thehackernews.com/2025/12/new-react-rsc-vulnerabilities-enable.html

MALWARE

GHOSTPOSTER — CAMPAÑA MALICIOSA VÍA EXTENSIONES DE FIREFOX UTILIZA ESTEGANOGRAFÍA EN PNG

Investigadores de Koi Security identificaron una nueva campaña maliciosa denominada GhostPoster, la cual ha comprometido a más de 50.000 usuarios de Mozilla Firefox mediante extensiones aparentemente legítimas. La campaña emplea técnicas avanzadas de esteganografía, ofuscación y carga en memoria, evadiendo controles de seguridad tradicionales y revisiones de los marketplaces oficiales.

Resumen técnico:

- Tipo de amenaza: Malware en extensiones de navegador y Backdoor / Adware avanzado
- Vector de infección: Extensiones maliciosas de Firefox distribuidas a través de la tienda oficial
- Técnica principal: Esteganografía en archivos PNG y carga de payload en memoria
- Usuarios afectados: Más de 50.000 instalaciones confirmadas

- Extensiones implicadas: Al menos 17 extensiones (VPN, traductores, clima, bloqueadores de anuncios, utilidades)
- Plataformas impactadas: Mozilla Firefox (usuarios finales y entornos corporativos)
- Ocultación del payload: Código JavaScript incrustado en los bytes de iconos PNG de las extensiones
- Evasión de detección: No descarga ejecutables externos, no escribe archivos maliciosos en disco y activación diferida (hasta varios días)
- Proceso de decodificación: Intercambio de mayúsculas y minúsculas, sustitución de caracteres numéricos ('8' ↔ '9'), decodificación Base64 y cifrado XOR dinámico en memoria usando el ID de la extensión.
- Comunicación C2: Infraestructura centralizada compartida por todas las extensiones y recuperación intermitente del payload para evadir análisis dinámico.
- Capacidades del malware: Ejecución remota de comandos dentro del navegador, inyección de scripts de seguimiento, eliminación de cabeceras de seguridad (CSP, X-Frame-Options), secuestro de tráfico web y enlaces de afiliados, fraude publicitario y de clics y persistencia mediante retardos y activación aleatoria.

Impacto potencial:

- Compromiso de la privacidad del usuario
- Manipulación del tráfico web
- Exposición a ataques adicionales (XSS, clickjacking)
- Riesgo elevado en entornos corporativos sin control de extensiones

Recomendaciones de mitigación:

1. Eliminar extensiones no esenciales, especialmente VPN gratuitas.
2. Instalar únicamente extensiones de desarrolladores verificados.
3. Auditar extensiones instaladas en entornos corporativos.
4. Restringir el uso de extensiones mediante políticas de navegador.
5. Mantener Firefox y el sistema operativo actualizados.
6. Implementar soluciones de seguridad con análisis de comportamiento.

Prioridad: Urgente.

Ampliar información:

- https://blog.elhacker.net/2025/12/nuevo-ataque-ghostposter-infecta-50000.html
- https://blog.segu-info.com.ar/2025/12/extensiones-de-navegador-maliciosas.html
- https://www.redeszone.net/noticias/seguridad/navegador-firefox-amenaza-roba-datos-evitar/
- https://ciberseguridadegalicia.gal/es/actualidad/noticias/nueva-campana-maliciosa-ghostposter-infecta-mas-de-50000-usuarios-de-firefox-mediante-iconos-png

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

EXPOSICIÓN MASIVA DE DATOS PROFESIONALES POR BASE DE DATOS MONGODB SIN AUTENTICACIÓN

Investigadores de seguridad identificaron una base de datos MongoDB expuesta públicamente en Internet sin ningún tipo de autenticación, la cual contenía miles de millones de registros con información profesional y corporativa. El incidente vuelve a evidenciar los riesgos derivados de configuraciones inseguras en servicios de bases de datos accesibles desde la red pública.

Resumen técnico:

- Tipo de incidente: Exposición de base de datos por configuración insegura
- Volumen de información expuesta: 16,14 TB de datos, aproximadamente 4.300 millones de registros y 9 colecciones.
- Origen de los datos: Información profesional recopilada principalmente de perfiles de LinkedIn y procesos automatizados de scraping y enriquecimiento de datos B2B.
- Información comprometida: Direcciones de correo electrónico, números de teléfono, cargos y relaciones profesionales, historial laboral y educativo, ubicación, idiomas y habilidades, enlaces a redes sociales y fotografías de perfil.

Impacto potencial:

- Campañas de phishing altamente dirigidas.
- Fraude por suplantación de identidad (CEO fraud).
- Ingeniería social avanzada contra organizaciones.
- Enriquecimiento de perfiles con filtraciones previas.
- Riesgos de privacidad para usuarios finales y empresas.

Recomendaciones para mitigar el riesgo:

1. Restringir el acceso a bases de datos expuestas en Internet.
2. Implementar autenticación y control de acceso en MongoDB.
3. Auditar servicios accesibles públicamente.
4. Monitorear posibles abusos derivados de filtraciones previas.
5. Sensibilizar a usuarios sobre campañas de phishing dirigidas.

Prioridad: Importante.

Ampliar Información:

- https://computerhoy.20minutos.es/ciberseguridad/filtracion-masiva-expone-4-300-millones-perfiles-profesionales-datos-contacto_6910230_0.html
- https://blog.segu-info.com.ar/2025/12/filtracion-masiva-expone-4300-millones.html
- https://digitalinside.es/exposicion-de-mas-de-4-000-millones-de-registros-profesionales-nos-muestra-la-problematica-de-las-bases-de-datos-sin-proteger/