GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4725

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	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

CVE-2025-58034 — FORTINET FORTIWEB — INYECCIÓN DE COMANDOS DEL SISTEMA OPERATIVO

Fortinet confirmó una vulnerabilidad de inyección de comandos del sistema operativo en FortiWeb que está siendo explotada activamente. La falla permite que un atacante autenticado ejecute comandos no autorizado mediante solicitudes HTTP manipuladas o comandos CLI maliciosos, comprometiendo directamente la integridad del dispositivo. Ha sido clasificada como CWE-78 (OS Command Injection) y afecta múltiples ramas del producto.

Resumen técnico:

- Vulnerabilidad identificada como CVE-2025-58034, CVSS 6.7 (Media).
- Tipo: OS Command Injection (CWE-78).
- Explotada activamente en el mundo real, confirmada por Fortinet y CISA (agregada al catálogo KEV).
- Requiere sesión autenticada, pero permite ejecutar comandos arbitrarios en el sistema operativo.
- Explotación mediante solicitudes HTTP o comandos CLI especialmente manipulados.
- Falla se debe a validación insuficiente de entradas en componentes clave de FortiWeb.
- No se detalló código vulnerable ni endpoints exactos.
- Publicada oficialmente por Fortinet el 18 de noviembre de 2025 (FG-IR-25-513).
- **Versiones afectadas:**
- FortiWeb 8.0: 8.0.0 – 8.0.1
- FortiWeb 7.6: 7.6.0 – 7.6.5
- FortiWeb 7.4: 7.4.0 – 7.4.10
- FortiWeb 7.2: 7.2.0 – 7.2.11
- FortiWeb 7.0: 7.0.0 – 7.0.11

Impacto potencial:

- Ejecución arbitraria de comandos en el sistema subyacente.
- Compromiso total del firewall de aplicaciones web.
- Riesgo de manipulación de configuraciones, exfiltración de datos e instalación de backdoors.
- Posible movimiento lateral hacia la red interna corporativa.
- Persistencia mediante modificación del sistema o abuso de cuentas administrativas existentes.

Recomendaciones de mitigación:

1. Actualizar de inmediato a las versiones corregidas: 8.0.2+, 7.6.6+, 7.4.11+, 7.2.12+, 7.0.12+.
2. Revisar y auditar cuentas administrativas y sesiones activas.
3. Limitar el acceso al panel administrativo únicamente desde redes internas confiables.
4. Implementar autenticación multifactor (MFA) para accesos privilegiados.
5. Revisar logs de administración en busca de solicitudes HTTP o comandos inusuales.

Prioridad: Crítica.

Ampliar información:

- https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20251119
- https://fortiguard.fortinet.com/psirt/FG-IR-25-513
- https://thehackernews.com/2025/11/fortinet-warns-of-new-fortiweb-cve-2025.html
- https://blog.segu-info.com.ar/2025/11/otra-vulnerabilidad-en-fortiweb-ahora.html

CVE-2025-13223 — GOOGLE CHROME V8 — TYPE CONFUSION Y EJECUCIÓN REMOTA DE CÓDIGO (ZERO-DAY EXPLOTADO ACTIVAMENTE)

Google lanzó un parche de emergencia para corregir una vulnerabilidad de Type Confusion en el motor V8 de Chrome que está siendo explotada activamente. La falla permite a un atacante remoto ejecutar código arbitrario mediante páginas HTML especialmente manipuladas, afectando a todas las plataformas principales (Windows, Linux y macOS). Es uno de los zero-day más relevantes del año.

Resumen técnico:

- Identificada como CVE-2025-13223, CVSS 8.8 (Alta).
- Vulnerabilidad de Type Confusion en el motor JavaScript y WebAssembly V8.
- Permite corrupción del heap y ejecución remota de código (RCE) mediante HTML malicioso.
- Explotación activa confirmada por Google, detectada por el equipo TAG el 12 de noviembre de 2025.
- Afecta versiones de Chrome anteriores a 142.0.7444.175/176.
- Este Zero-day es el séptimo explotado en Chrome este año y el tercero de Type Confusion en V8 durante 2025.
- Actualización también corrige la vulnerabilidad relacionada CVE-2025-13224, descubierta por IA Big Sleep (no explotada).
- Riesgo extendido al ecosistema Chromium (Edge, Brave, Opera, Vivaldi).

Impacto potencial:

- Ejecución remota de código al visitar sitios web maliciosos.
- Compromiso del navegador y acceso a sesiones, cookies y credenciales.
- Descarga e instalación silenciosa de malware (spyware, ransomware, stealers).
- Compromiso total del endpoint en usuarios sin parche aplicado.
- Exposición masiva debido a la popularidad global de Chrome y derivados.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a Chrome: Windows/Linux: 142.0.7444.175 o 142.0.7444.176 y MacOS: 142.0.7444.176
2. Forzar manualmente la actualización: Menú > Ayuda > Información de Google Chrome.
3. Reiniciar el navegador para aplicar el parche.
4. Verificar y aplicar parches en navegadores basados en Chromium (Edge, Brave, Opera, Vivaldi).
5. Habilitar actualizaciones automáticas y reforzar protección contra sitios maliciosos.
6. Precaución ante phishing que simule "actualizaciones urgentes" de Chrome.

Prioridad: Crítica.

Ampliar información:

- https://thehackernews.com/2025/11/google-issues-security-fix-for-actively.html
- https://www.q2bstudio.com/nuestro-blog/166349/google-lanza-parche-para-vulnerabilidad-zero-day-en-chrome-protege-tu-navegador-ahora-con-esta-actualizacion

- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-zero-day-en-google-chrome-activamente-explotada/
- https://unaaldia.hispasec.com/2025/11/alerta-de-seguridad-google-lanza-parche-critico-para-un-zero-day-en-chrome-explotado-activamente-cve-2025-13223.html
- https://blog.segu-info.com.ar/2025/11/zero-day-explotado-activamente-en.html

CVE-2025-12762 — PGADMIN4 (HASTA LA VERSION 9.9) — EJECUCIÓN REMOTA DE CÓDIGO MEDIANTE ARCHIVOS PLAIN MANIPULADOS (RCE CRÍTICA)

Se identificó una vulnerabilidad crítica de ejecución remota de código (RCE) en pgAdmin4, la interfaz open source usada ampliamente para gestionar bases de datos PostgreSQL en entornos corporativos. El fallo, presente en versiones hasta la 9.9, permite a un atacante ejecutar comandos arbitrarios en el servidor aprovechando restauraciones en modo servidor (server mode) a partir de archivos PLAIN manipulados, comprometiendo directamente la infraestructura de base de datos.

Resumen técnico:

- Identificada como CVE-2025-12762, con severidad Crítica, CVSS v3.1: 9.3 / 10.
- Falla asociada a CWE-94 — Improper Control of Code Generation (Code Injection).
- Se origina en la falta de sanitización al procesar archivos de respaldo PLAIN-format durante restauraciones en modo servidor (server mode).
- Un usuario autenticado con privilegios bajos puede inyectar comandos arbitrarios construyendo un dump malicioso.
- Exploitable con acceso de red y sin interacción del usuario.
- Afecta todas las instalaciones de pgAdmin4 en modo servidor en versiones ≤ 9.9, comunes en entornos empresariales.
- Corrección implementada en el commit 1d39739 y liberada en pgAdmin 10.0.

Impacto potencial:

- Ejecución remota de código en el servidor que aloja pgAdmin4.
- Compromiso completo de bases de datos PostgreSQL administradas desde la instancia afectada.
- Riesgo de movimiento lateral hacia sistemas dependientes.
- Fuga o manipulación de información crítica almacenada en bases de datos.
- Alto impacto en entornos donde se procesan dumps externos o automatizados en pipelines DevOps.

Recomendaciones de mitigación:

1. Actualizar inmediatamente a pgAdmin4 versión 10.0 o superior.
2. Deshabilitar restauraciones en formato PLAIN cuando no sean estrictamente necesarias.
3. Limitar el acceso a la función de restauración solo a usuarios altamente confiables.
4. Auditar accesos y privilegios asociados a administración PostgreSQL.
5. Implementar sanitización estricta en pipelines de DevOps que manipulen dumps de bases de datos.
6. Revisar sistemas expuestos a archivos provenientes de terceros o integraciones externas.

Prioridad: Crítica.

Ampliar información:

- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-rce-en-pgadmin4-permite-ejecucion-remota-de-codigo/
- https://cybersecuritynews.com/pgadmin4-vulnerability/
- https://cybersecurityinsight.us/index.php/en/cyb-threat/critical-rce-flaw-in-pgadmin4-exposes-database-servers

MALWARE

TUONI C2 FRAMEWORK — USADO EN CAMPAÑA DE INGENIERÍA SOCIAL CONTRA SECTOR INMOBILIARIO (IN-MEMORY PAYLOADS Y STEALTH C2)

Investigadores revelaron una campaña dirigida contra una empresa inmobiliaria en EE. UU. que utilizó Tuoni, un framework de comando y control (C2) relativamente nuevo que ofrece capacidades avanzadas de ejecución en memoria. Aunque diseñado para actividades de

red team, su versión gratuita ("Community Edition") ha facilitado su adopción por actores maliciosos.

Resumen técnico:

- Campaña observada en octubre de 2025, con acceso inicial mediante ingeniería social vía Microsoft Teams.
- El atacante induce al usuario a ejecutar un comando PowerShell que descarga un segundo script desde kupaoquan[.]com.
- El loader utiliza esteganografía en un archivo BMP para ocultar un payload de segunda fase.
- El payload extrae y ejecuta shellcode en memoria, resultando en la carga de TuoniAgent.dll.
- El agente establece comunicación con el C2 (kupaoquan[.]com), permitiendo control remoto y persistencia.
- Se identificaron indicios de generación de código asistida por IA en el loader inicial (comentarios y estructura modular).
- Tuoni C2 se publicó inicialmente en 2024 y cuenta con versión gratuita que facilita su uso indebido.
- Diseño modular orientado a in-memory operations y evasión mediante protocolos cifrados.

Impacto potencial:

- Ejecución remota de payloads sin tocar disco (low forensic footprint).
- Compromiso completo de endpoints mediante comunicación persistente con el C2.
- Riesgo de escalación lateral en entornos corporativos tras el acceso inicial.

- Abuso de herramientas de red team para operaciones ofensivas reales.
- Difusión facilitada por ingeniería social y loaders de bajo perfil.

Recomendaciones de mitigación:

1. Restringir y monitorear comunicaciones vía Microsoft Teams para prevenir ataques de impersonación.
2. Bloquear y monitorear indicadores asociados (dominios, hosts, hashes).
3. Implementar EDR con detección de carga de shellcode in-memory y anomalías en PowerShell.
4. Deshabilitar ejecución de scripts no firmados y aplicar políticas de AppLocker/WDAC.
5. Capacitación del personal frente a campañas de ingeniería social que emplean "Teams Spoofing".
6. Evaluar riesgos derivados del uso interno de herramientas de red team con versiones gratuitas o sin control.

Prioridad: Urgente.

Ampliar información:

- https://www.antifraude.co/investigadores-revelan-el-papel-clave-del-comando-y-control-tuoni-c2-en-ciberataques-avanzados/
- https://thehackernews.com/2025/11/researchers-detail-tuoni-c2s-role-in.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

EXPLOTACIÓN ACTIVA DE MÚLTIPLES VULNERABILIDADES EN FORTINET FORTIWEB

Fortinet enfrenta una situación crítica luego de que se confirmara la explotación activa de dos vulnerabilidades en su línea FortiWeb, en medio de cuestionamientos por la divulgación tardía y la aplicación de parches silenciosos que dificultaron la respuesta oportuna de los equipos de seguridad.

Resumen técnico:

- La vulnerabilidad CVE-2025-64446 en FortiWeb es de tipo path traversal (CWE-23) y permite a un atacante no autenticado enviar solicitudes HTTP/HTTPS manipuladas para acceder a un ejecutable CGI interno y ejecutar comandos administrativos.
- La vulnerabilidad CVE-2025-58034, también en FortiWeb, es de tipo OS command injection (CWE-78) y permite a un atacante autenticado —una vez comprometida una cuenta o mediante explotación encadenada— ejecutar comandos arbitrarios del sistema operativo mediante peticiones HTTP o comandos CLI diseñados.
- Ambas fallas afectan múltiples ramas de versiones (por ejemplo 8.0.0-8.0.1, 7.6.x, etc) y han sido confirmadas como explotadas en el mundo real; además, la primera fue incluida en el catálogo de vulnerabilidades explotadas reconocidas por Cybersecurity and Infrastructure Security Agency (KEV) el 14 de noviembre.

Impacto potencial:

- Un atacante sin credenciales puede lograr acceso administrativo completo al dispositivo FortiWeb afectado, lo que le permite modificar configuración, crear cuentas administrativas, desactivar o modificar reglas de seguridad del WAF, y comprometer otras partes de la red protegida por el appliance.
- La explotación de estos dispositivos de seguridad (WAF) implica que un componente que debería proteger el perímetro quede comprometido, lo que multiplica el riesgo para toda la infraestructura de aplicaciones web de la organización.
- Dada la observación de exploit públicos, inclusión en el catálogo KEV y disponibilidad de módulo Metasploit para la primera vulnerabilidad, el riesgo para organizaciones que no parcheen es inmediato.
-
- **Recomendaciones para mitigar el riesgo:**

1. Aplicar de inmediato las versiones corregidas proporcionadas por Fortinet (por ejemplo, en la rama 8.0 actualizar a 8.0.2 o superior) para todos los productos FortiWeb afectados.
2. En caso de que no sea viable la actualización urgente, deshabilitar HTTP/HTTPS para interfaces de gestión expuestas a Internet y restringir acceso administrativo del dispositivo a redes internas confiables.
3. Auditar las configuraciones del dispositivo: revisar logs de creación de cuentas nuevas, modificación de perfiles de acceso, actividad inusual en la consola de administración, y confirmar que no existen cuentas administrativas sospechosas o cambios inesperados.
4. Monitorizar el tráfico de red hacia el dispositivo WAF, buscando patrones atípicos o conexiones salientes hacia dominios desconocidos, y habilitar detección de intrusión/endpoint (EDR) para interceptar comandos inusuales en los appliances de seguridad.

5. Integrar estos fallos en el plan de gestión de vulnerabilidades y asegurarse de que los parches de seguridad críticos con explotación activa sean priorizados sin demora.

Prioridad: Urgente.

Ampliar Información:

- https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/
- https://www.cybersecuritydive.com/news/critical-vulnerability-in-fortinet-fortiweb-is-under-exploitation/805688/
- https://www.cisa.gov/news-events/alerts/2025/11/14/fortinet-releases-security-advisory-relative-path-traversal-vulnerability-affecting-fortiweb
- https://thehackernews.com/2025/11/fortinet-fortiweb-flaw-actively.html