GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2825

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

VULNERABILIDADES

Vulnerabilidad SQLI no autenticada en FortiWeb (CVE-2025-25257, FG-IR-25-151)

Fortinet ha emitido un aviso urgente para corregir una vulnerabilidad crítica de inyección de SQL no autenticada en su WAF FortiWeb, identificada como CVE-2025-25257 y FG-IR-25-151.

Resumen técnico:

- CVE-2025-25257 (CVSS 9.6/10): Un atacante remoto sin autenticación puede inyectar comandos SQL en el endpoint /api/fabric/device/status mediante solicitudes HTTP/HTTPS maliciosas. El problema radica en la inserción directa del token Bearer en la consulta SQL sin sanitización.
- La inyección SQL permite:
  - Ejecución de cualquier comanda SQL.

  - Extracción o manipulación de datos de configuración.
  - Escritura arbitraria en archivos vía INTO OUTFILE.
  - Potencial ejecución de código, aprovechando scripts CGI como ml-draw.py y módulos Python con capacidad de ejecución.
- Afecta versiones:
  - 7.6.0–7.6.3
  - 7.4.0–7.4.7
  - 7.2.0–7.2.10
  - 7.0.0–7.0.10

Impacto potencial

- Control completo de FortiWeb, ya que se ejecutan comandos sin autenticación.
- Exposición de credenciales y datos confidenciales.
- Posible escalada a acceso de sistema operativo, comprometiendo la red protegida por el WAF.
- Exposición relevante: más de 5 000 instancias conectadas a Internet detectadas por Shodan.

Recomendaciones:

1. Actualizar de inmediato a versiones parcheadas:
   - 7.6 → 7.6.4+
   - 7.4 → 7.4.8+
   - 7.2 → 7.2.11+
   - 7.0 → 7.0.11+
2. Como mitigación temporal, desactivar acceso HTTP/HTTPS al GUI administrativo.
3. Monitorear registros del WAF para detectar patrones de inyección SQL o actividad anómala en el endpoint mencionado.
4. Implementar reglas de IPS/WAF específicas que bloqueen inyecciones SQL en /api/fabric/device/status.

5. Auditoría continua y escaneo urbano con herramientas como Qualys (QIDs 44706, 732762) o sistemas nacionales (Cert EU, CCB Bélgica, CSA Singapur)

Prioridad: Crítica.

Ampliar Información:

- https://www.cisecurity.org/advisory/a-vulnerability-in-fortiweb-could-allow-for-sql-injection_2025-063
- https://threatprotect.qualys.com/2025/07/14/fortinet-fortiweb-unauthenticated-sql-injection-vulnerability-cve-2025-25257/
- https://cert.europa.eu/publications/security-advisories/2025-024/pdf

Ejecución remota de código en aplicaciones Laravel debido a APP_KEY filtradas

Investigadores de GitGuardian y Synacktiv han identificado un grave riesgo de ejecución remota de código (RCE) en aplicaciones Laravel expuestas por la filtración de sus claves APP_KEY en repositorios públicos.

Resumen técnico:

- Laravel genera una clave APP_KEY de 32 bytes usada para cifrado, firmas y producción de tokens. Si esta clave se filtra (por ejemplo, en .env en GitHub), se vuelve un vector de ataque eficaz.
- Entre 2018 y mayo de 2025, GitGuardian extrajo más de 260.000 APP_KEYs públicas y encontró 600 aplicaciones vulnerables.
- Cuando SESSION_DRIVER=cookie, Laravel utiliza decrypt() automáticamente, lo que puede desencadenar deserialización insegura y permitir a un atacante ejecutar código arbitrario si posee la clave filtrada. Esta vulnerabilidad originalmente fue CVE-2018-15133 y persiste en varios entornos actuales como CVE-2024-55556.

- Se detectaron aproximadamente 650.000 instancias Laravel conectadas públicamente; de estas, más de 400 aplicaciones eran potencialmente explotables

Impacto potencial:

- Ejecución remota de código en el servidor de la aplicación.
- Exfiltración de datos sensibles, acceso administrativo, instalación de malware o puertas traseras.
- Riesgo real en entornos donde los desarrolladores usan .env con APP_KEY en repositorios públicos o imágenes Docker accesibles.

Recomendaciones:

1. Rotar inmediatamente las APP_KEY filtradas y cambiar cualquier secret conectado.
2. Revisar y limpiar todos los repositorios Git, imágenes Docker e históricos CI/CD para eliminar secretos expuestos.
3. Evitar SESSION_DRIVER=cookie. Preferir file, database u otros drivers seguros.
4. Implementar una herramienta de escaneo de secretos, como GitGuardian o similares, para prevenir futuras filtraciones.
5. En proyectos Laravel, revisar que APP_DEBUG=false en producción y restringir archivos. env del repositorio.
6. Adoptar buenas prácticas de seguridad en PHP/Laravel: validación de entradas, escape de salida, permisos correctos de archivos .env, actualizaciones regulares y pruebas de penetración.

Prioridad: Crítica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/07/aplicaciones-laravel-expuestas-la.html

VMware corrige cuatro zero-days en ESXi tras explotación en Pwn2Own Berlin 2025 (CVE-2025-41236, 41237, 41238, 41239)

VMware publicó parches críticos para múltiples productos —ESXi, Workstation, Fusion y VMware Tools— que fueron comprometidos en el concurso Pwn2Own Berlin 2025 mediante vulnerabilidades día-cero.([turn0search0])(turn0search3)

Detalles técnicos:

- CVE-2025-41236–*Integer overflow* en adaptador VMXNET3
  Permite a código con privilegios dentro de una *VM* (máquina virtual) ejecutar instrucciones en el sistema host. Reportado por Nguyen Hoang Thach (STARLabs SG).([turn0search0])(turn0search4).

- CVE-2025-41237–*Integer underflow* en VMCI
  Un ataque que provoca escritura fuera de rangos permitidos ('out-of-bounds write') cuando una VM interactúa con el host, permitiendo ejecución de código local. Reportado por Corentin BAYET (REverse Tactics).([turn0search0])(turn0search4).

- CVE-2025-41238–*Heap overflow* en controlador Paravirtual SCSI (PVSCSI)
  Bloque de memoria no controlado permite que un administrador de VM ejecute código en el proceso VMX del host. Reportado por Synacktiv.([turn0search0])(turn0search4)

- CVE-2025-41239–Fuga de información en VMware Tools (Windows)
  Permite a una VM recuperar datos sensibles del host, usada combinada con CVE-41237. Reportado por Corentin BAYET.([turn0search0])(turn0search3)

Impacto potencial:

- CVE-41239 Exposición de datos del host.
- Permiten que un atacante con acceso administrador a una VM controle el entorno del hypervisor.
- Riesgo en entornos de multitenencia, laboratorios o nubes privadas.

Recomendaciones:

- Aplicar parches inmediatamente mediante VMSA-2025-0013.(ver ESXi, Workstation, Fusion, Tools)
- Actualizar VMware Tools en sistemas Windows para mitigar fuga de datos.
- Reiniciar hosts y sistemas virtualizados tras la aplicación del parche.
- Monitorear logs de VMX y VMCI para detectar actividad maliciosa en VMs.
- Revisar políticas de aislamiento VM/host y considerar desactivar adaptadores VMXNET3 o PVSCSI en entornos sensibles hasta actualizar.

Prioridad: Urgente.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/vmware-fixes-four-esxi-zero-day-bugs-exploited-at-pwn2own-berlin/
- https://www.securityweek.com/vmware-flaws-that-earned-hackers-340000-at-pwn2own-patched/
- https://blogs.vmware.com/security/2025/05/vmware-and-pwn2own-2025-berlin.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

Ola de variantes maliciosas de ASYNCRAT tras liberar el código abierto

El código fuente de AsyncRAT, un troyano de acceso remoto (RAT) escrito en C#, se publicó en GitHub en 2019. Su diseño modular ha permitido que aparezcan más de 30 variantes y forks sofisticados, que incluyen desde burlas como *SantaRAT* hasta amenazas graves como DcRat y VenomRAT.

Resumen técnico:

- Arquitectura modular y de plugins: Permite a distintos desarrolladores crear versiones personalizadas (forks) con características como keylogging, captura de pantalla, robo de credenciales o cifrado de archivos.
- Evasión avanzada: Variantes como *DcRat* y *VenomRAT* implementan técnicas como el bypass de AMSI/ETW, módulos integrados de ransomware, control de servicios y robo de tokens de Discord.
- Forks “creativos”: *NonEuclidRAT* añade funciones como USB spreading, clipper de criptomonedas, geolocalización y plugins “de broma” (por ejemplo, sustos

visuales); *JasonRAT* envía datos según la región, *XieBroRAT* integra Cobalt Strike y robo de credenciales en navegadores.

- Distribución masiva: Utilizado en campañas de phishing, malvertising y cracks con loaders como GuLoader o SmokeLoader, infectando decenas de miles de máquinas en el último año.
- Malware-as-a-Service: Existen builders y módulos preconfigurados a la venta en Telegram y foros de la dark web, facilitando la creación de variantes sin necesidad de conocimientos avanzados.

Impacto potencial:

- Robo de información: credenciales, tokens, grabaciones de escritorio.
- Acceso remoto persistente: Apex total del sistema, instalación de malware adicional como ransomware.
- Evasión de detección: técnicas anti-análisis bloqueando AMSI/ETW, rutas ofuscadas y módulos polimórficos.
- Ataques dirigidos y automatizados: múltiples variantes permiten adaptarse a objetivos específicos y pasar desapercibidos frente a firmas conocidas.

Recomendaciones:

1. Detección centrada en comportamiento: implementar EDR/XDR y monitorear actividad inusual como uso de cargadores o comunicación con C2.
2. Bloquear herramientas de ofuscación y loaders: restringir ejecución de GuLoader, SmokeLoader y monitorear descargas desde dominios sospechosos.
3. Política estricta de plugins y DLLs: controlar qué extensiones y módulos se cargan en sistemas críticos.
4. Revisar logs de red y procesos: identificar conexiones cifradas sospechosas (Cloudflare, DGA) y ejecución de RATs.

5. Formación continua: alertar a usuarios sobre phishing y evitar descargar software o extensiones de orígenes no fiables.

Prioridad: Crítica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/07/codigo-abierto-de-asyncrat-desata-una-peligrosa-ola-mundial-de-variantes-sigilosas.html
- https://thehackernews.com/2025/07/asyncrats-open-source-code-sparks-surge.html
- https://cyberscoop.com/asyncrat-malware-variants-eset/
- https://blog.segu-info.com.ar/2025/07/troyano-de-codigo-abierto-asyncrat.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

CO-OP confirma el robo de datos de 6,5 millones de miembros en un ciberataque

El CO-OP, una de las mayores cooperativas de consumo del Reino Unido, confirmó que en un ciberataque ocurrido en abril de 2025 se robaron los datos personales de 6.5 millones de sus miembros. La información comprometida incluye nombres, direcciones, números de teléfono, correos electrónicos y fechas de nacimiento, pero no datos financieros ni historiales de transacciones.

El ataque fue sofisticado: los atacantes lograron acceso tras un ataque de ingeniería social que les permitió resetear la contraseña de un empleado y moverse lateralmente dentro de la red, llegando a robar el archivo NTDS.dit del dominio Windows, que contiene hashes de contraseñas. Se relaciona con el grupo de ciberdelincuentes Scattered Spider, vinculado también a ataques previos contra Marks & Spencer y Harrods.

Como respuesta, CO-OP tuvo que apagar varios sistemas, lo que afectó operaciones internas y servicios como tiendas y funerarias, aunque mantuvieron abiertas las tiendas al público. La empresa notificó a sus miembros y está trabajando con agencias de seguridad y expertos para mitigar el impacto y evitar futuros incidentes.

Además, CO-OP ha iniciado una alianza con The Hacking Games para fomentar la formación en ciberseguridad entre jóvenes, buscando convertir el incidente en una oportunidad para promover carreras éticas en el sector.

Si quieres, puedo ayudarte a analizar las posibles vulnerabilidades explotadas en este ataque o a preparar recomendaciones para mitigar riesgos similares

Prioridad: Importante.

Ampliar Información:

- https://diginomica.com/turns-out-65-million-co-op-members-had-their-personal-data-nicked-time-some-socially-pleasing

- https://www.bleepingcomputer.com/news/security/co-op-confirms-data-of-65-million-members-stolen-in-cyberattack/
- https://www.techerati.com/news-hub/co-op-confirms-personal-data-of-6-5-million-members-stolen/

Interrupción global de Cloudflare 1.1.1.1 por error de configuración — no se debió a ataque ni BGP HIJACK

El servicio DNS público 1.1.1.1 de Cloudflare sufrió una interrupción global el 14 de julio de 2025 entre las 21:48 y 22:54 UTC. Cloudflare confirmó que fue causada por un error interno de configuración, y no por un ataque ni secuestro de rutas BGP

Resumen técnico:

- Una configuración realizada el 6 de junio como parte de un proyecto "Data Localization Suite" (DLS) vinculó erróneamente los prefijos de 1.1.1.1 a una ubicación no productiva.
- El 14 de julio a las 21:48 UTC, se agregó una ubicación de prueba al entorno, lo que provocó un refresco integral de la configuración de enrutamiento BGP. Esto retiró temporalmente los anuncios BGP de los rangos 1.1.1.0/24, 1.0.0.0/24 y sus equivalentes IPv6, dejando el servicio inaccesible.
- Cloudflare detectó el problema a las 22:01 UTC, revirtió la configuración a las 22:20 UTC y restauró el servicio plenamente a las 22:54 UTC.
- Algunos usuarios confundieron el incidente con un supuesto secuestr o BGP porque se detectó un anuncio malicioso puntual por parte de un tercer operador (Tata Communications), pero no estuvo relacionado con la causa real.

Impacto:

- 1.1.1.1, 1.0.0.1, y rangos IPv6 quedaron inalcanzables globalmente, inutilizando la resolución DNS para miles de millones de usuarios.

- Los usuarios de otros servicios DNS (por ejemplo, 1.1.1.1/DOH vía cloudflare-dns.com) no se vieron afectados.
- El incidente provocó interrupciones en navegadores, apps y servicios conectados a internet durante más de una hora.

Recomendaciones:

1. Añadir redundancia DNS: combinar 1.1.1.1 con otra solución pública (como 8.8.8.8 o 9.9.9.9) para garantizar servicio continuo.
2. Monitorizar resoluciones DNS en infraestructuras críticas para detectar caídas.
3. Evaluar riesgos de dependencia de un solo proveedor y considerar arquitecturas DNS híbridas o georredundantes.
4. Mantener actualizados los mecanismos de Anycast/BGP y las herramientas de alertas asociadas al enrutamiento DNS.

Prioridad: Importante.

Ampliar Información:

- https://www.bleepingcomputer.com/news/security/cloudflare-says-1111-outage-not-caused-by-attack-or-bgp-hijack/
- https://blog.cloudflare.com/cloudflare-1-1-1-1-incident-on-july-14-2025/
- https://www.theregister.com/2025/07/16/cloudflare_fesses_up_to_config