GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1025

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

VULNERABILIDADES

SQLI autenticado en CLI

El aviso de seguridad FG-IR-24-130 publicado por FortiGuard Labs informa sobre una vulnerabilidad de inyección SQL autenticada en la interfaz de línea de comandos (CLI) de ciertos productos Fortinet, identificada como CVE-2024-33501. Esta vulnerabilidad se debe a una neutralización inadecuada de elementos especiales en comandos SQL, lo que podría permitir a un atacante autenticado ejecutar comandos SQL arbitrarios en el sistema afectado.

Para mitigar esta vulnerabilidad, se recomienda actualizar los productos afectados a las versiones corregidas proporcionadas por Fortinet. Además, es aconsejable seguir las mejores prácticas de seguridad, como limitar el acceso a la CLI a usuarios autorizados y monitorear regularmente los sistemas para detectar actividades sospechosas.

Prioridad: Urgente.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-130

Vulnerabilidad asociada a máquinas virtuales

El aviso de seguridad FG-IR-24-305 emitido por FortiGuard Labs aborda una vulnerabilidad identificada como CVE-2024-52960, relacionada con la aplicación inadecuada de medidas de seguridad del lado del cliente en la funcionalidad de descarga de máquinas virtuales (VM).

Esta vulnerabilidad podría permitir que usuarios malintencionados eludan las restricciones de seguridad implementadas en el servidor, aprovechando controles insuficientes en el lado del cliente. Para mitigar este riesgo, se recomienda encarecidamente actualizar los productos afectados a las versiones corregidas proporcionadas por Fortinet y seguir las mejores prácticas de seguridad para garantizar la protección de los sistemas.

Prioridad: Urgente.

Ampliar Información:

https://www.fortiguard.com/psirt/FG-IR-24-305

Elastic lanza una solución urgente para vulnerabilidad crítica de Kibana que permite la ejecución remota de código

Elastic ha lanzado actualizaciones de seguridad para abordar una vulnerabilidad crítica en Kibana, identificada como CVE-2025-25012, con una puntuación CVSS de 9.9. Esta vulnerabilidad de "prototype pollution" permite la ejecución de código arbitrario mediante

la carga de archivos especialmente diseñados y solicitudes HTTP específicas. Afecta a todas las versiones de Kibana desde la 8.15.0 hasta la 8.17.3, y se ha solucionado en la versión 8.17.3.

En las versiones de Kibana entre la 8.15.0 y la 8.17.0, la vulnerabilidad puede ser explotada por usuarios con el rol de "Viewer". En las versiones 8.17.1 y 8.17.2, se requiere que los atacantes tengan privilegios más avanzados, incluyendo acceso a los roles "fleet-all", "integrations-all" y "actions:execute-advanced-connectors". Elastic recomienda encarecidamente actualizar a la versión 8.17.3 o posterior para mitigar este riesgo. Como medida adicional, se sugiere deshabilitar la función "Integration Assistant" configurando "xpack.integration_assistant.enabled: false" en el archivo de configuración de Kibana ("kibana.yml") para minimizar la exposición a la vulnerabilidad.

Prioridad: Crítico.

Ampliar Información:

https://thehackernews.com/2025/03/elastic-releases-urgent-fix-for.html

---

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Paquete malicioso de PyPI roba claves privadas de Ethereum

Investigadores de ciberseguridad han identificado un paquete malicioso en el repositorio de Python Package Index (PyPI) llamado set-utils, diseñado para robar claves privadas de Ethereum de las víctimas. Este paquete, que ha sido descargado 1.077 veces antes de ser eliminado del repositorio oficial, se hacía pasar por bibliotecas populares como python-utils y utils, engañando a desarrolladores desprevenidos para que lo instalaran y, consecuentemente, permitieran a los atacantes acceder a sus billeteras de Ethereum.

El paquete malicioso estaba dirigido a desarrolladores y organizaciones que trabajan con aplicaciones blockchain basadas en Python, especialmente aquellas que utilizan bibliotecas de gestión de billeteras como eth-account. El código malicioso interceptaba funciones de creación de billeteras, como from_key() y from_mnemonic(), para capturar las claves privadas generadas en el sistema comprometido. Lo notable de este ataque es que las claves privadas robadas se exfiltraban mediante transacciones en la cadena de bloques a través del endpoint Polygon RPC, lo que dificultaba su detección por métodos tradicionales que monitorean solicitudes HTTP sospechosas.

Prioridad: Urgente.

https://thehackernews.com/2025/03/this-malicious-pypi-package-stole.html

---

Microsoft advierte sobre una campaña de publicidad maliciosa

Microsoft ha identificado una campaña de malvertising a gran escala que ha afectado a más de un millón de dispositivos en todo el mundo, diseñada para robar información sensible. Detectada a principios de diciembre de 2024 y rastreada bajo el nombre Storm-0408, la campaña se originó en sitios web de streaming ilegales con redireccionadores

maliciosos que llevaban a sitios intermedios, desde donde los usuarios eran redirigidos a plataformas como GitHub, Discord y Dropbox, utilizadas para alojar y distribuir malware.

El proceso de infección es complejo y consta de múltiples etapas, incluyendo el uso de malware como Lumma Stealer y Doenerium para recopilar información del sistema. Además, se emplearon herramientas como NetSupport RAT y scripts de AutoIT para facilitar el robo de datos adicionales. Los atacantes también utilizaron scripts de PowerShell para descargar malware adicional, identificar aplicaciones instaladas y buscar carteras de criptomonedas, lo que indica un posible robo de datos financieros.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/03/microsoft-warns-of-malvertising.html

---

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

La IA facilita el fraude de identificación de personas

La inteligencia artificial (IA) ha emergido como una herramienta que facilita el fraude de identidad, permitiendo a los ciberdelincuentes ser más eficientes en sus actividades ilícitas. Según informe, más de un tercio de los líderes de riesgo e innovación bancaria en el Reino Unido, España y Estados Unidos consideran que el incremento del fraude potenciado por IA y deepfakes es su mayor desafío actual.

Los delincuentes emplean diversas tácticas basadas en IA, como la apropiación fraudulenta de cuentas mediante imitaciones de audio y video para eludir verificaciones de identidad, la falsificación de documentos digitales y la creación de identidades sintéticas combinando datos reales e inventados. Estas técnicas han incrementado la sofisticación y frecuencia de los ataques, afectando tanto a individuos como a instituciones de distintos sectores.

Prioridad: Importante

Ampliar Información:

https://blog.segu-info.com.ar/2025/03/la-ia-facilita-el-fraude-de.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000

Blind Eagle ataca instituciones colombianas usando fallas de NTLM, RAT y ataques basados en GitHub

El grupo de amenazas conocido como Blind Eagle, activo desde al menos 2018 y también identificado como APT-C-36, ha estado llevando a cabo campañas dirigidas contra instituciones colombianas y entidades gubernamentales desde noviembre de 2024. Estas

campañas han afectado a más de 1.600 víctimas, incluyendo instituciones judiciales y otras organizaciones gubernamentales y privadas en Colombia.

Blind Eagle utiliza tácticas de ingeniería social, como correos electrónicos de spear-phishing, para obtener acceso inicial a los sistemas objetivo. Posteriormente, despliega troyanos de acceso remoto (RAT) como AsyncRAT, NjRAT, Quasar RAT y Remcos RAT. Recientemente, han explotado una variante de la vulnerabilidad CVE-2024-43451 de Windows, adoptado un servicio de empaquetado llamado HeartCrypt y distribuido sus cargas útiles a través de plataformas como Bitbucket y GitHub, además de Google Drive y Dropbox.

Un análisis del repositorio de GitHub de Blind Eagle reveló una posible ubicación en la zona horaria UTC-5, que coincide con varios países de América del Sur. Además, se descubrió un archivo que contenía combinaciones de cuentas y contraseñas de 1.634 direcciones de correo electrónico únicas, incluyendo nombres de usuario, contraseñas, correos electrónicos, contraseñas de correo electrónico y PINs de cajeros automáticos asociados con individuos, agencias gubernamentales, instituciones educativas y empresas que operan en Colombia.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/03/blind-eagle-hacks-colombian.html