GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

# Boletín de Ciberseguridad Semanal

Edición °4424

# 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** | 0 | 1 | 1 |
| **NOTICIAS DE CIBERSEGURIDAD** | 0 | 0 | 2 |

# VULNERABILIDADES

## Vulnerabilidad crítica en Fortimanager bajo explotación activa

Fortinet ha advertido sobre una vulnerabilidad crítica identificada como CVE-2024-47575, que afecta a las versiones de FortiManager entre 7.2.2 y 7.4.1. Esta vulnerabilidad permite a atacantes no autenticados ejecutar comandos a través de solicitudes diseñadas específicamente, lo que compromete la seguridad de los sistemas afectados. La vulnerabilidad está siendo explotada activamente por el grupo de amenazas UNC5820, que ha aprovechado esta debilidad para atacar organizaciones a nivel global.

Para mitigar los riesgos, Fortinet ha lanzado parches de seguridad y recomienda a los administradores de sistemas actualizar las versiones vulnerables de FortiManager inmediatamente. Además, se sugiere implementar certificados personalizados y reforzar las políticas de seguridad locales para prevenir accesos no autorizados. La CISA ha

destacado la urgencia de aplicar las actualizaciones antes del 13 de noviembre de 2024, añadiendo este CVE a su catálogo de vulnerabilidades activamente explotadas.

**Prioridad:** 1 critico.

**Ampliar información:**

https://thehackernews.com/2024/10/fortinet-warns-of-critical.html

---

## Vulnerabilidad en AWS CDK expone a secuestro de cuentas

Se descubrió una vulnerabilidad en AWS Cloud Development Kit (CDK) que expone a los usuarios a riesgos de secuestro de cuentas. Aunque aún no se ha asignado un CVE específico, la falla permite a atacantes realizar "namesquatting" al predecir nombres de buckets S3, lo que les permite inyectar plantillas maliciosas y obtener acceso no autorizado a los recursos.

AWS corrigió el problema en la versión 2.149.0 del CDK. Se recomienda actualizar inmediatamente a la última versión, evitar el uso de nombres predecibles para los buckets y reforzar las políticas de acceso a través de AWS IAM para minimizar los riesgos de explotación. Además, es aconsejable realizar auditorías frecuentes de las configuraciones de seguridad y limitar los privilegios de acceso solo a personal esencial.

**Prioridad:** 1 Crítico.

**Ampliar información:**

https://thehackernews.com/2024/10/aws-cloud-development-kit-vulnerability.html

---

## Nvidia corrige vulnerabilidades críticas en controladores de Windows y Linux

Nvidia ha lanzado parches para corregir varias vulnerabilidades graves en sus controladores gráficos, con CVE´s que van desde CVE-2024-0117 hasta CVE-2024-0128.

Estas vulnerabilidades permiten a los atacantes ejecutar código malicioso, escalar privilegios, causar denegación de servicio y acceder a recursos no autorizados, lo que afecta tanto los controladores gráficos en Windows y Linux como el software de virtualización de GPU (vGPU).

Para mitigar estos riesgos, Nvidia ha publicado actualizaciones en varias versiones de controladores. En Windows, las versiones seguras son R535 (535.113.01), R531 (531.79) y R528 (528.89). En Linux, las actualizaciones recomendadas son R535 (535.113.01) y R470 (470.199.02). Se recomienda a los usuarios aplicar estos parches de inmediato y revisar las configuraciones de seguridad en sus sistemas.

**Prioridad:** 2 urgente.

**Ampliar información:**

https://www.securityweek.com/nvidia-patches-high-severity-flaws-in-windows-linux-graphics-drivers/

---

## Recomendaciones generales sobre vulnerabilidades:

Para reducir las vulnerabilidades en los sistemas, se sugieren las siguientes acciones clave:

Aplicar parches de seguridad de forma regular para solucionar fallos conocidos.

Añadir una capa adicional de seguridad, como la autenticación de dos factores (2FA), para complicar el acceso no autorizado.

Restringir los permisos de usuarios y aplicaciones, limitando el acceso solo a lo necesario para reducir riesgos.

Utilizar herramientas de detección de intrusiones para monitorizar y detectar comportamientos sospechosos.

Estas medidas son esenciales para contribuir a fortalecer la seguridad de los sistemas.

## MALWARE

### Nuevas variantes del malware bancario Grandoreiro mejoran técnicas de evasión

El malware bancario Grandoreiro, rastreado por Kaspersky, ha evolucionado, incorporando técnicas avanzadas para evadir la detección. Se propaga principalmente a través de correos electrónicos de phishing y anuncios maliciosos en Google, atacando a más de 1,700 instituciones financieras en 45 países. Este troyano bancario utiliza técnicas como el seguimiento de movimientos del mouse y algoritmos de generación de dominios para eludir la detección, permitiendo a los atacantes robar credenciales y realizar fraudes financieros.

Además, Grandoreiro implementa tácticas anti-análisis para frustrar a los investigadores de seguridad, como la detección de entornos de prueba. Para mitigar el riesgo, se recomienda actualizar el software de seguridad, evitar enlaces sospechosos y utilizar autenticación multifactor en todas las cuentas bancarias.

**Prioridad:** 2 urgente.

**Ampliar información:**

https://thehackernews.com/2024/10/new-grandoreiro-banking-malware.html

---

### El malware Latrodectus se vuelve más popular entre los ciberdelincuentes

El malware Latrodectus, detectado por Forcepoint, está siendo utilizado cada vez más por el grupo criminal LunarSpider, asociado con WizardSpider. Este malware se propaga principalmente a través de correos electrónicos de phishing con archivos PDF o HTML maliciosos, que al abrirse permiten la descarga de software malicioso en los sistemas infectados. Latrodectus tiene la capacidad de robar datos sensibles y establecer puertas

traseras para ataques futuros, lo que lo convierte en una herramienta peligrosa para el espionaje y el robo de información.

El malware es particularmente preocupante debido a su capacidad para pasar desapercibido en las etapas iniciales de la infección. Para mitigar el riesgo, se recomienda no abrir archivos enlaces sospechosos, implementar filtros avanzados de correo electrónico, y mantener actualizado el software de seguridad en todos los dispositivos.

**Prioridad:** 3 importante.

**Ampliar información:**

https://www.securityweek.com/latrodectus-malware-increasingly-used-by-cybercriminals/

---

## Recomendaciones generales sobre malware:

Para protegerse del malware, es fundamental:

Mantener el software y los sistemas operativos actualizados de manera regular, ya que los atacantes suelen aprovechar vulnerabilidades en versiones obsoletas.

Utilizar programas antivirus y antimalware confiables, asegurándose de que siempre estén actualizados.

Activar la autenticación multifactor (MFA) para asegurar cuentas sensibles y dificultar el acceso no autorizado.

Ser cauteloso con correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de infección por malware.

Hacer copias de seguridad periódicas de los archivos importantes, para evitar pérdidas en caso de ataques como el ransomware.

Restringir los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

## NOTICIAS DE CIBERSEGURIDAD

### El malware Bumblebee resurge tras operativos policiales

Después del desmantelamiento de infraestructuras criminales en la "Operación Endgame", Bumblebee ha reaparecido, según informes de Netskope. Este malware se propaga principalmente mediante correos electrónicos de phishing que contienen archivos ZIP con archivos LNK maliciosos. Al abrirse, estos archivos ejecutan comandos de PowerShell que instalan malware a través de instaladores disfrazados de software legítimo.

Bumblebee es altamente sofisticado, lo que lo convierte en una amenaza crítica para organizaciones. Se recomienda evitar abrir archivos sospechosos, actualizar regularmente el software de seguridad, y educar a los empleados sobre cómo identificar intentos de phishing.

**Prioridad:** 3 importante.

**Ampliar información:**

https://www.securityweek.com/bumblebee-malware-loader-resurfaces-following-law-enforcement-takedown/

---

### Apple crea entorno virtual para mejorar la ciberseguridad en la nube privada

Apple ha lanzado un entorno de investigación virtual (VRE) para ayudar a los investigadores de seguridad a identificar vulnerabilidades en su tecnología Private Cloud Compute (PCC), que se utiliza para procesar datos confidenciales en la nube con cifrado de extremo a extremo. Este entorno proporciona acceso a componentes internos clave del sistema, permitiendo que los expertos simulen fallos potenciales en un entorno controlado. La

iniciativa busca mejorar la seguridad de este sistema utilizado para procesar datos de inteligencia artificial.

Apple, que identificó la necesidad de un entorno de pruebas seguro, ha ofrecido recompensas de hasta $1 millón a quienes descubran vulnerabilidades graves. Con este programa, se recomienda a los investigadores que exploren este entorno y reporten cualquier fallo potencial, lo que no solo mejorará la seguridad de la infraestructura de Apple, sino que también contribuirá al fortalecimiento de la ciberseguridad en servicios en la nube.

**Prioridad:** 3 importante.

**Ampliar información:**

https://www.bleepingcomputer.com/news/apple/apple-creates-private-cloud-compute-vm-to-let-researchers-find-bugs/