GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1224

En alianza con

TD SYNNEX FORTINET

BOLETIN 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	2	0
MALWARE	0	1	5
NOTICIAS DE CIBERSEGURIDAD	0	1	9

VULNERABILIDADES

QNap advierte sobre un error critico de omisión de autenticación en sus dispositivos NAS

QNAP ha emitido una advertencia sobre vulnerabilidades presentes en sus productos de software NAS, los cuales incluyen QTS, QuTS hero, QuTScloud y myQNAPcloud, dichas vulnerabilidades, podrían permitir a atacantes acceder a los dispositivos. El fabricante taiwanés de almacenamiento adjunto a la red (NAS) ha identificado tres vulnerabilidades potenciales que podrían resultar en la omisión de autenticación, la inyección de comandos y la inyección de SQL.

Prioridad: 1 Crítico.

Ampliar información:

https://www.qnap.com/en/security-advisory/qsa-24-09

Una falla critica de Fortinet puede afectar a 150.000 dispositivos expuestos

Análisis en la web pública revela que aproximadamente 150,000 dispositivos Fortinet FortiOS y FortiProxy que protegen la web, son vulnerables al CVE-2024-21762, una vulnerabilidad crítica que permite la ejecución de código sin autorización. La Agencia de Seguridad Cibernética e Infraestructura de Estados Unidos (CISA, por sus siglas en inglés) confirmó el mes pasado que los atacantes están explotando activamente esta falla al incluirla en su catálogo de vulnerabilidades conocidas explotadas (KEV).

Prioridad: 2 Urgente.

Ampliar información:

https://securityaffairs.com/160224/hacking/fortios-bug-cve-2024-21762-150k-evices.htML

PoC para vulnerabilidades críticas de Arcserve UDP publicada (CVE-2024-0799, CVE-2024-0800)

Arcserve ha abordado vulnerabilidades críticas de seguridad (CVE-2024-0799, CVE-2024-0800) en su Solución de Protección de Datos Unificada (UDP), que podrían encadenarse para cargar archivos maliciosos en el sistema operativo subyacente de Windows. Los investigadores de Tenable han publicado un script de explotación que demuestra el ataque.

Prioridad: 2 Urgente.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/14/cve-2024-0799-cve-2024-0800

Vulnerabilidades críticas del complemento ChatGPT exponen datos confidenciales

Se han descubierto tres vulnerabilidades de seguridad en las funciones de extensión utilizadas por ChatGPT, las cuales abren la puerta al acceso no autorizado a cuentas y servicios de usuarios, incluidos repositorios confidenciales en plataformas como GitHub. Los complementos de ChatGPT, así como las versiones personalizadas publicadas por desarrolladores, amplían las capacidades del modelo de IA, permitiendo interacciones con servicios externos mediante el acceso generativo al chatbot de IA de OpenAI y permisos para ejecutar tareas en varios sitios web de terceros, incluyendo GitHub y Google Drive. Estas tres vulnerabilidades críticas fueron descubiertas por investigadores de Salt Labs, siendo la primera de ellas durante la instalación de nuevos complementos, cuando ChatGPT redirige a los usuarios a sitios web de complementos para la aprobación del código.

Prioridad: 1 Crítico.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/critical-chatgpt-plugin-vulnerabilities-expose-sensitive-data

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.

- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

Correo Medusa Ransomware continúa atacando a los distritos escolares de Estados Unidos

El equipo de investigación de amenazas de SonicWall Capture Labs ha estado rastreando el ransomware que ha ganado reciente notoriedad, conocido como Medusa. Medusa surgió como una plataforma de ransomware como servicio (RaaS) a finales de 2022. El grupo detrás de Medusa propaga predominantemente este malware a través de vulnerabilidades en programas sin parches, dirigiendo sus ataques a diversos sectores industriales como tecnología, educación, manufactura, atención médica y comercio minorista.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/03/medusa-ransomware-continues-attacks-on-us-school-districTS

Piratas informáticos aprovechan la falla del complemento de WordPress para infectar 3.300 sitios con malware

Los piratas informáticos están comprometiendo sitios de WordPress al aprovechar una vulnerabilidad en versiones obsoletas del complemento Popup Builder, lo que ha llevado a la infección de más de 3.300 sitios web con código malicioso. La vulnerabilidad explotada en estos ataques se conoce como CVE-2023-6000 y se trata de una vulnerabilidad de secuencias de comandos entre sitios (XSS) que afecta a las versiones de Popup Builder 4.2.3 o anteriores. Esta vulnerabilidad fue inicialmente revelada en noviembre de 2023.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/03/android-adware-hidden-behind-the-facade-of-gaming-icon

---

BianLian opta por PowerShell después de la explotación de TeamCity

Desde que Avast lanzó un descifrador para BianLian en enero de 2023, el grupo ha cambiado su enfoque hacia operaciones exclusivamente de extorsión. Desde entonces, el Equipo de Investigación e Inteligencia de GuidePoint (GRIT) ha estado vigilando de cerca las actividades de BianLian. En colaboración con el equipo DFIR de GuidePoint, se respondió a un incidente que comenzó con la explotación de un servidor TeamCity, lo que resultó en la implementación de una puerta trasera GO de BianLian mediante PowerShell.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/03/bianlian-threat-actors-exploiting.html

---

Infostealer disfrazado de instalador de Adobe Reader

El Centro de Inteligencia de Seguridad de AhnLab (ASEC) descubrió recientemente la distribución de un ladrón de información que se hace pasar por un instalador de Adobe Reader. El actor de amenazas está distribuyendo el archivo como un PDF, lo que solicita a los usuarios descargar y ejecutar el archivo.

Prioridad: 2 Urgente.

Ampliar información:

https://asec.ahnlab.com/en/62853/

Phishing a través de Venmo

Venmo es una de las aplicaciones de pago más populares en todo el mundo. Como propiedad de PayPal, ofrece una manera sencilla para que amigos envíen dinero entre sí. Además, muchas empresas también utilizan esta plataforma y su función de red social agrega otra dimensión a la experiencia. Sin embargo, es importante tener en cuenta que el recibo de correos electrónicos con malware o phishing pone en riesgo la seguridad de esta aplicación. En el tercer trimestre de 2023, el valor total de los pagos realizados a través de esta, alcanzó los 68 mil millones de dólares, representando un crecimiento interanual del 7%. Según Statista, Venmo se encuentra entre las tres principales marcas de pagos en los Estados Unidos.

Prioridad: 3 Importante.

Ampliar información:

https://blog.checkpoint.com/harmony-email/phishing-through-venmo

---

Registradores de pulsaciones de teclas, software espía y ladrones dominan las detecciones de malware para PYMES

En 2023, el 50% de las detecciones de malware dirigidas a las PYMES consistieron en keyloggers, spyware y ladrones de información, según Sophos. Estos tipos de malware son utilizados por los atacantes para robar datos y credenciales valiosas. Posteriormente, los atacantes pueden utilizar esta información robada para obtener acceso remoto no autorizado, extorsionar a las víctimas, implementar ransomware y llevar a cabo otras acciones maliciosas. El informe de Sophos también examina a los Intermediarios de Acceso Inicial (IAB), delincuentes que se especializan en violar redes informáticas.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/13/smbs-ransomware-cyberthreat

---

Recomendaciones generales sobre malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.

- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.
- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

La estrategia de ciberseguridad requiere la colaboración CISO-CFO

La cuantificación del riesgo cibernético combina la experiencia técnica del CISO con el enfoque del CFO en el impacto financiero para desarrollar una comprensión más completa y sólida de las implicaciones que se encuentran en juego.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/cyber-risk/cyber-insurance-strategy-requires-ciso-cfo-collaboration

---

Cómo los ciberpartisanos bielorrusos están librando una guerra digital contra dos dictadores

No es común que los grupos de hackers tengan fuertes inclinaciones políticas, pero para el grupo cibernético bielorruso Partisanos, cuyo objetivo es derrocar el régimen autoritario de su país, esta inclinación es más una necesidad que una elección. El grupo forma parte del

movimiento de oposición más amplio en Bielorrusia, que ha ganado atención global después de las protestas masivas de 2020 contra los resultados de las elecciones nacionales, que fueron manipulados por el dictador respaldado por Rusia, Alexander Lukashenko.

Prioridad: 3 Importante.

Ampliar información:

https://therecord.media/belarusian-cyber-partisans-operations-politics-russia-ukraine

---

La IA Gemini de Google es vulnerable a la manipulación de contenidos

Al igual que ChatGPT y otras herramientas GenAI, Gemini es susceptible a ataques que pueden provocar la divulgación de mensajes del sistema, revelar información confidencial y ejecutar acciones potencialmente maliciosas.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/cyber-risk/google-gemini-vulnerable-to-content-manipulation-researchers-say

---

Las 10 principales vulnerabilidades de aplicaciones web en 2021-2023

Ayudar a las empresas a navegar por el mundo de las vulnerabilidades de las aplicaciones web y proteger las suyas propias es una tarea crucial. Para abordar este desafío, la comunidad en línea Open Web Application Security Project (OWASP) creó el Top Ten de OWASP, una lista de las diez vulnerabilidades más críticas en aplicaciones web.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/top-vulnerabilities-corporate-web

---

El talento de ransomware surge en Akira después de la desaparición de lockbit

¿Sería LockBit tan severo bajo cualquier otro nombre? Los grupos de ransomware de habla rusa pueden cambiar de nombre y operar bajo diferentes marcas, pero las personas involucradas a menudo se unen detrás de cualquier entidad que siga siendo una empresa en funcionamiento. Por lo tanto, se informó sobre el flujo de los mejores talentos de LockBit, que recientemente fue interrumpido por las fuerzas del orden, a Akira, que aparentemente está activo.

Prioridad: 3 Importante.

Ampliar información:

https://www.bankinfosecurity.com/ransomware-talent-surges-to-akira-after-lockbits-demise-a-24583

Informe de amenazas de Sophos 2024: ciberdelincuencia en la calle principal

El ciberdelito afecta a personas de todos los ámbitos de la vida, pero tiene un impacto desproporcionado en las pequeñas empresas. Aunque los ciberataques a grandes

empresas y agencias gubernamentales reciben mucha atención mediática, las pequeñas empresas (generalmente definidas como organizaciones con menos de 500 empleados) suelen ser más vulnerables a los ciberdelincuentes y sufren las consecuencias de manera más severa. La falta de personal experimentado en operaciones de seguridad, la inversión insuficiente en ciberseguridad y los presupuestos más reducidos para tecnología en general son factores que contribuyen a este nivel de vulnerabilidad. Cuando son víctimas de ciberataques, el costo de la recuperación puede ser tan elevado que incluso puede llevar al cierre de muchas pequeñas empresas.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/cyber-incident-victims-small

---

Los líderes de TI piensan que el almacenamiento de datos inmutable es una póliza de seguro contra secuestro de datos

Los líderes de TI consideran que el almacenamiento inmutable es esencial en la lucha contra los ciberataques, según Scality. Las organizaciones ahora reconocen que las amenazas de ransomware son inevitables. Los informes indican que una de cada cuatro organizaciones que pagan un rescate nunca recupera sus datos, y solo el 16% logra recuperarlos sin pagar un rescate.

Prioridad: 3 Importante.

Ampliar información:

https://www.helpnetsecurity.com/2024/03/14/immutable-storage-cybersecurity-strategy

---

Por qué los actores de amenazas DDoS están cambiando sus tácticas

Con una historia que abarca más de 25 años, los ataques DDoS no son, a primera vista, nada nuevo. Sin embargo, bajo la superficie, hay un paisaje en rápida evolución con avances significativos. Los métodos de ataque se han diversificado y los atacantes pueden ahora dirigirse a objetivos individuales, como servidores, o a redes enteras simultáneamente. Esta caja de herramientas en constante expansión ha hecho que los ataques DDoS sean mucho más accesibles, incluso disponibles como servicio para comprar en línea.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/opinions/ddos-threat-actors-tactics

---

Investigadores exponen errores de configuración de Microsoft SCCM que se pueden utilizar en ataques cibernéticos

Investigadores de seguridad han creado un repositorio de conocimientos sobre técnicas de ataque y defensa basadas en configuraciones incorrectas del Administrador de Configuración de Microsoft (MCM), lo que podría permitir que un atacante ejecute cargas útiles o se convierta en un controlador de dominio. El Administrador de Configuración (anteriormente conocido como System Center Configuration Manager o SCCM, ConfigMgr) existe desde 1994 y está presente en muchos entornos de Active Directory, ayudando a los administradores a gestionar servidores y estaciones de trabajo en una red Windows.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/researchers-expose-microsoft-sccm-misconfigs-usable-in-cyberattacks

---

Intercambiadores de SIM secuestran números de teléfono en ataques de eSIM

Los intercambiadores de SIM han adaptado sus ataques para robar el número de teléfono de un objetivo transfiriéndolo a una nueva tarjeta eSIM, una SIM digital almacenada en un chip regrabable presente en muchos modelos recientes de teléfonos inteligentes. Los módulos de identidad de suscriptor integrados (eSIM) son tarjetas digitales almacenadas en el chip del dispositivo móvil que cumplen la misma función y propósito que una tarjeta SIM física, pero pueden ser reprogramadas y reaprovisionados de forma remota, desactivadas, intercambiadas o eliminadas.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/sim-swappers-hijacking-phone-numbers-in-esim-attacks

---