GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3923

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	3	3	
MALWARE	1	4	1
NOTICIAS DE CIBERSEGURIDAD	1	1	3

VULNERABILIDADES

Vulnerabilidades en Firmware BMC IPMI de Supermicro exponen Servidores

Supermicro ha lanzado actualizaciones de firmware BMC IPMI para abordar múltiples vulnerabilidades que afectan a modelos selectos de placas base. Estos problemas (rastreados como CVE-2023-40284 a CVE-2023-40290) podrían permitir que atacantes remotos obtengan acceso de root al sistema BMC. Las vulnerabilidades incluyen tres problemas de scripting entre sitios (XSS) en el frontend del servidor BMC, que podrían ser explotados de forma remota sin autenticación para ejecutar código JS arbitrario, y una vulnerabilidad de inyección de comandos en el backend del servidor BMC. Aunque Supermicro ha dado una calificación CVSS de 7.2 a 8.3 a estas vulnerabilidades, Binarly las considera de gravedad crítica y ha señalado que un atacante necesitaría cierta información previa para explotarlas con éxito.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/new-supermicro-bmc-vulnerabilities-could-expose-many-servers-to-remote-attacks/

Apple Advierte sobre la Explotación de Nueva Vulnerabilidad Zero-Day en el Kernel de iOS 17

Apple ha lanzado una actualización de seguridad para iOS que resuelve dos vulnerabilidades críticas, una de las cuales ya ha sido explotada en ataques reales. La vulnerabilidad del kernel conocida como CVE-2023-42824 permitía a atacantes locales elevar sus privilegios en el sistema. Este incidente marca el decimosexto ataque zero-day registrado en la plataforma iOS de Apple. Además, la actualización aborda una vulnerabilidad relacionada con un desbordamiento de búfer en WebRTC.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/apple-warns-of-newly-exploited-ios-17-kernel-zero-day/

Qualcomm Parchea 3 Zero-Days Reportados por Google

Qualcomm ha anunciado parches de seguridad para más de dos docenas de vulnerabilidades en sus productos, incluyendo tres zero-days reportados por unidades de ciberseguridad de Google. Aunque no se han compartido detalles sobre los ataques que podrían haber aprovechado estas vulnerabilidades, el hecho de que hayan sido reportadas por Google sugiere que podrían haber sido explotadas por vendedores comerciales de spyware. La mayoría de las vulnerabilidades restantes, descubiertas internamente por Qualcomm, se consideran de gravedad crítica o alta y afectan a módems, firmware WLAN y productos automotrices, incluyendo problemas de memoria y divulgación de información.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/qualcomm-patches-3-zero-days-reported-by-google/

Vulnerabilidades Críticas en TorchServe Podrían Exponer Infraestructura de IA

Un conjunto de vulnerabilidades críticas en una herramienta llamada TorchServe podría permitir a actores de amenazas tomar el control completo de servidores que forman parte de la infraestructura de inteligencia artificial (IA) de algunas de las empresas más grandes del mundo, según una empresa de ciberseguridad. Estas vulnerabilidades podrían comprometer por completo su infraestructura de IA, permitiendo a los atacantes ver, modificar, robar y eliminar modelos de IA que a menudo contienen la propiedad intelectual central de un negocio.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/critical-torchserve-flaws-could-expose-ai-infrastructure-of-major-companies/

Vulnerabilidad de Microsoft Office Word permite la ejecución de código JavaScript

Una reciente vulnerabilidad descubierta en Microsoft Office Word ha generado preocupaciones sobre la seguridad de esta popular suite de productividad. Clasificada como una vulnerabilidad de Cross-Site Scripting (XSS), permite a los atacantes ejecutar código JavaScript arbitrario en documentos de Word. La vulnerabilidad radica en cómo Office maneja el título de los videos incrustados en los documentos, lo que podría permitir a los atacantes inyectar código malicioso cuando se reproduce un video en un documento de Word. Esto subraya la importancia de mantener el software actualizado y ser cauteloso con el contenido incrustado en los documentos para evitar posibles riesgos de seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/microsoft-office-xss-flaw/

Vulnerabilidad 'Looney Tunables' en Linux permite a atacantes obtener privilegios de root

Se ha revelado una vulnerabilidad en la Biblioteca C GNU (glibc) que afecta a sistemas Linux y que ha sido apodada "Looney Tunables". Esta vulnerabilidad, identificada como CVE-2023-4911, se encuentra en la versión 2.34 de glibc y podría permitir a atacantes locales obtener privilegios de root en sistemas vulnerables. La vulnerabilidad está relacionada con la variable de entorno GLIBC_TUNABLES y su manipulación maliciosa puede causar un desbordamiento de búfer y corrupción de memoria en el cargador dinámico ld.so de glibc. La explotación de esta vulnerabilidad podría tener un impacto significativo en la seguridad, la fiabilidad y el rendimiento del sistema en numerosas distribuciones de Linux. Se recomienda a los administradores de sistemas que apliquen los parches de seguridad correspondientes para proteger sus sistemas contra esta amenaza potencialmente grave.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/looney-tunables-linux-vulnerability/

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

Balada Injector: Una Amenaza Emergente para Temas Premium de WordPress

Se ha identificado una amenaza en aumento conocida como Balada Injector que se dirige a sitios web que utilizan temas premium de tagDiv, como Newspaper y Newsmag, así como a los administradores de WordPress. Esta amenaza se aprovecha de una reciente vulnerabilidad de XSS almacenada sin autenticación en el complemento tagDiv Composer. La situación resalta la importancia de la seguridad en línea para los usuarios de estos temas y los administradores de WordPress.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.sucuri.net/2023/10/balada-injector-targets-unpatched-tagdiv-plugin-newspaper-theme-wordpress-admins.html?web_view=true

Continúa la Distribución de Ransom Knight y Remcos a pesar del Golpe a la Infraestructura de Qakbot

A pesar del desmantelamiento de la infraestructura de Qakbot por parte del FBI, los actores de amenazas afiliados continúan distribuyendo el malware Ransom Knight y la puerta trasera Remcos a través de correos electrónicos de phishing desde principios de agosto de 2023. Esta actividad persistente sugiere que la operación policial no ha afectado la capacidad de entrega de spam de los operadores de Qakbot, lo que plantea la posibilidad de que reconstruyan su infraestructura en el futuro, representando una amenaza continua para la ciberseguridad.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/?&web_view=true

---

GoldDigger: Nuevo troyano Android apunta a docenas de bancos vietnamitas

GoldDigger, un nuevo troyano Android, se ha centrado en el sector financiero de Vietnam, utilizando técnicas de evasión sofisticadas. Este malware se hace pasar por diversas aplicaciones y utiliza el Servicio de Accesibilidad de Android para robar credenciales bancarias y datos personales. Su capacidad para evitar la detección mediante software legítimo lo convierte en una amenaza preocupante en Asia Pacífico y destaca la importancia de soluciones de protección en tiempo real y análisis de comportamiento para contrarrestarlo.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/golddigger-new-android-trojan-targeting-dozens-of-vietnamese-banks-3a4000f9/?web_view=true/

BunnyLoader: Nuevo Malware como Servicio

Investigadores de Zscaler ThreatLabz han descubierto BunnyLoader, un nuevo malware como servicio (MaaS) que se ha anunciado en varios foros de cibercriminales desde septiembre de 2023. Este cargador de malware, escrito en C/C++, se vende por $250 con licencia de por vida. Además, se encuentra en constante desarrollo, con actualizaciones que añaden nuevas funciones y solucionan errores. BunnyLoader utiliza técnicas anti-sandbox y de evasión para descargar o ejecutar cargas secundarias, robar información sensible, criptomonedas, ejecutando también, comandos remotos.

Prioridad: 2 Urgente.

Ampliar información:

- hhttps://securityaffairs.com/151869/malware/bunnyloader-maas.html

---

Descargas Falsas de Thunderbird Distribuyen Ransomware

Mozilla emitió una advertencia sobre sitios web maliciosos que ofrecen descargas de Thunderbird después de que un grupo de ransomware utilizara esta técnica para distribuir malware. El grupo Snatch ransomware ha estado utilizando anuncios pagados de Google para disfrazar su malware como aplicaciones populares como Adobe Reader, Discord, Microsoft Teams y Mozilla Thunderbird. Mozilla aconseja a los usuarios que solo descarguen Thunderbird desde sitios web de confianza. La cuota de mercado de Thunderbird es pequeña, pero aun así representa un riesgo para muchas personas y organizaciones.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/mozilla-warns-of-fake-thunderbird-downloads-delivering-ransomware/

Storm-0324 Abusa de Microsoft Teams para Obtener Acceso Inicial y Desplegar Ransomware

El grupo de amenazas financieras Storm-0324 ha sido detectado utilizando mensajes de phishing a través de Microsoft Teams como método para obtener acceso inicial y desplegar ransomware. Este grupo ha estado previamente relacionado con ataques de ransomware y distribución de malware. Utilizan mensajes de phishing con temáticas de facturación para engañar a los usuarios y luego entregan un cargador malicioso JSSLoader, una vez que logran acceso, facilitan el acceso a otros grupos de ransomware. Esta táctica representa una nueva forma de ataque basada en Teams y se considera altamente peligrosa.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/storm-0324-abusing-microsoft-teams/

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

Alerta por Ataques de LockBit 3.0 Black y BlackCat/AlphV: Riesgos de Ransomware

LockBit 3.0 Black y BlackCat/AlphV, dos grupos de ciberdelincuentes que han vuelto a la escena en las últimas semanas. Estos grupos utilizan ransomware para cifrar los datos de las víctimas y luego exigen un rescate para descifrarlos. Los investigadores destacan la importancia de tomar medidas para protegerse contra estos ataques, incluido evitar el acceso RDP expuesto, y señalan que las tecnologías heurísticas y de comportamiento pueden ser efectivas para bloquear estos tipos de ataques de ransomware.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/151855/malware/lockbit-3-0-black-blackcat-alphv.html/

Fundación Linux presenta OpenPubkey, un protocolo criptográfico de código abierto para fortalecer la seguridad de la cadena de suministro

Linux anuncia OpenPubkey, un protocolo criptográfico de código abierto diseñado para fortalecer la seguridad de la cadena de suministro. Desarrollado como parte del producto de acceso de infraestructura de confianza cero de BastionZero, OpenPubkey se integra ahora con Docker. Su objetivo es permitir la vinculación de claves criptográficas a usuarios y cargas de trabajo al convertir un proveedor de identidad OpenID Connect en una autoridad de certificación.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/linux-foundation-announces-openpubkey-open-source-cryptographic-protocol/

Sony Confirma Robo de Datos en Dos Ataques de Hackers Recientes

Sony ha compartido información sobre dos recientes ataques de piratería informática llevados a cabo por grupos de ransomware conocidos, RansomedVC y Cl0p, aunque el impacto parece haber sido limitado en ambos casos. El primero afirmó haber comprometido todos los sistemas de Sony, pero la investigación reveló actividad no autorizada en un solo servidor de pruebas en Japón, sin indicios de acceso a datos de clientes o socios comerciales. El segundo incidente involucró la explotación de una vulnerabilidad zero-day en el software MOVEit de Progress Software por parte del grupo Cl0p, que afectó a miles de organizaciones y resultó en la exposición de información personal de empleados de Sony Interactive Entertainment y sus familiares, con medidas de monitoreo y restauración de identidad ofrecidas a los afectados.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/sony-confirms-data-stolen-in-two-recent-hacker-attacks/

Las 7 estrategias principales de seguridad de REST API para proteger sus Endpoints

En el paisaje actual impulsado por las API REST, es crucial implementar estrategias sólidas de seguridad para proteger estos puntos finales vitales. Las API REST son fundamentales para la comunicación entre clientes y servidores en aplicaciones web, pero su flexibilidad y apertura las exponen a diversas amenazas de seguridad. Para garantizar la integridad y confiabilidad de las API REST, se deben considerar estrategias como la limitación de operaciones verbales HTTP, el uso de

TLS (HTTPS), la autenticación de usuarios, la restricción de acceso a recursos, la limitación de velocidad, la validación de parámetros de entrada y pruebas de seguridad frecuentes.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/rest-api-security-strategies/

Hackers Utilizan Dropbox para Robar Credenciales de Microsoft SharePoint

En las primeras dos semanas de septiembre, se detectaron 5,440 ataques que utilizan Dropbox para crear páginas de inicio de sesión falsas y dirigir a las víctimas a sitios web de recolección de credenciales. Esta táctica, conocida como BEC 3.0, implica el uso de plataformas legítimas como Dropbox para enviar y alojar materiales de phishing, lo que dificulta enormemente su detección tanto para los servicios de seguridad de correo electrónico como para los usuarios finales. Estos ataques, que utilizan Dropbox para alojar páginas de recolección de credenciales, están en aumento y se están extendiendo a través de diversas plataformas de productividad, lo que los convierte en una amenaza significativa en el panorama de la ciberseguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/hackers-busing-dropbox/