GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0524

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	4	
MALWARE	1	3	1
NOTICIAS DE CIBERSEGURIDAD		2	3

VULNERABILIDADES

Actualización de Windows 11: soluciona problemas de audio Bluetooth y aborda 24 errores

Microsoft lanzó la vista previa de enero de 2024 para Windows 11 (versiones 22H2 y 23H2) a través de la actualización KB5034204. Esta actualización mensual opcional soluciona problemas de audio Bluetooth, incluyendo la pérdida de sonido en auriculares Bluetooth Low Energy (LE) durante la transmisión de música, así como inconvenientes con llamadas telefónicas Bluetooth. Además, se ocupó de problemas en la búsqueda del menú de inicio y en el controlador de fuentes OpenType. Los administradores pueden probar estas mejoras antes del lanzamiento oficial en febrero de 2024. La actualización también aborda problemas como bloqueos intermitentes del dispositivo y mejora la confiabilidad durante las transiciones de energía.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/microsoft/windows-11-kb5034204-update-fixes-bluetooth-audio-issues-24-bugs/?&web_view=true

---

Vulnerabilidad de alta severidad en Splunk Enterprise para Windows

Splunk ha abordado varias vulnerabilidades en Splunk Enterprise, incluida una de alta severidad (CVE-2024-23678) que afecta a las instalaciones en Windows. Esta falla podría permitir la ejecución de código malicioso debido a la deserialización insegura de datos no confiables. Se recomienda a los usuarios actualizar a las versiones 9.0.8, 9.1.3 o superiores. No se ha revelado si hay ataques en curso que aprovechen esta vulnerabilidad. Otras vulnerabilidades también fueron corregidas en esta actualización.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/158019/security/splunk-flaw-windows-installs.html?web_view=truel

---

Vulnerabilidad crítica en GoAnywhere MFT permite a cualquiera ser administrador

Se ha revelado una falla de seguridad crítica en el software GoAnywhere Managed File Transfer (MFT) de Fortra, que podría ser explotada para crear un nuevo usuario administrador. Identificado como CVE-2024-0204, el problema tiene un puntaje de CVSS de 9.8 sobre 10. La vulnerabilidad permite eludir la autenticación, posibilitando que un usuario no autorizado cree un usuario administrador a través del portal de administración. Se recomienda a los usuarios actualizar a la versión 7.4.1 o aplicar soluciones temporales, especialmente aquellos con instancias no contenerizadas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/patch-your-goanywhere-mft-immediately.html?&web_view=true

---

Apple emite parche para vulnerabilidad crítica de día cero en iPhones y Macs

Apple ha lanzado actualizaciones de seguridad para iOS, iPadOS, macOS, tvOS y el navegador web Safari para abordar una vulnerabilidad de día cero que está siendo activamente explotada. La falla, identificada como CVE-2024-23222, es un error de confusión de tipo en el motor de navegadores WebKit, que podría permitir la ejecución de código arbitrario al procesar contenido web maliciosamente diseñado. Se insta a los usuarios a actualizar sus dispositivos de inmediato para mitigar el riesgo de explotación. Además, se han aplicado correcciones para otras vulnerabilidades, incluidas algunas retro compatibles con versiones más antiguas de dispositivos.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/apple-issues-patch-for-critical-zero.html?&web_view=true

---

Vulnerabilidad en Apache Active MQ explotada en nuevos ataques con Godzilla Web Shell

Investigadores de ciberseguridad advierten sobre un "aumento notable" en la actividad de actores de amenazas que están explotando activamente una vulnerabilidad ya parcheada en Apache ActiveMQ para entregar el web shell Godzilla en hosts comprometidos. La vulnerabilidad CVE-2023-46604, que permite la ejecución remota de código, ha sido objeto de explotación activa desde su divulgación en octubre de 2023, utilizada por diversos adversarios para implementar ransomware, rootkits, mineros de criptomonedas y botnets de DDoS. En esta nueva serie de intrusiones observada por Trustwave, instancias vulnerables son atacadas con web shells basados en JSP que se ocultan

dentro de un formato binario desconocido, evitando la detección por parte de escáneres de seguridad y basados en firmas. La campaña destaca la importancia de actualizar a la última versión de Apache ActiveMQ para mitigar posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/apache-activemq-flaw-exploited-in-new.html?&web_view=true

---

Vulnerabilidad en Google Kubernetes expone más de 250,000 clústeres a control por cualquier usuario de Google

Una nueva vulnerabilidad, denominada "Sys:all", en Google Kubernetes Engine (GKE) permite que cualquier usuario de Google tome el control de clústeres Kubernetes mal configurados. Más de 250,000 clústeres GKE activos se ven afectados, incluyendo algunos con información sensible. La configuración incorrecta de los enlaces de control de acceso basado en roles (RBAC) otorga privilegios extremos a los grupos system:authenticated, posiblemente permitiendo el acceso y control por parte de cualquier titular de cuenta de Google. La explotación de esta vulnerabilidad tiene serias implicaciones, como el acceso a credenciales de AWS y datos operativos críticos. Se recomienda a los usuarios de GKE que actualicen a la última versión para mitigar posibles amenazas.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/google-kubernetes-flaw-cluster

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

Nuevo malware CherryLoader imita CherryTree para desplegar exploits

CherryLoader, un nuevo cargador de malware basado en Go, ha sido identificado por Arctic Wolf Labs. Este malware se hace pasar por la aplicación legítima CherryTree para engañar a los usuarios. Utilizado en al menos dos intrusiones recientes, CherryLoader descarga herramientas de elevación de privilegios, como PrintSpoofer o JuicyPotatoNG, para establecer persistencia en el dispositivo comprometido. Sorprendentemente, CherryLoader es modular y permite a los actores de amenazas cambiar exploits sin necesidad de recompilar el código, lo que aumenta su peligrosidad.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/new-cherryloader-malware-mimics.html?&web_view=true

---

La falsa solución: nuevo malware Chae$ 4.1 se oculta en descargas de controladores

La última versión del malware Chae$ 4.1 utiliza avanzada polimorfia de código para eludir la detección antivirus. Morphisec Threat Labs ha documentado sus hallazgos sobre Chae$ 4.1, destacando sus mecánicas, implicaciones y medidas de seguridad. El malware se propaga a través de un correo electrónico en portugués que simula ser una solicitud urgente de un abogado. Una vez descargado, Chae$ 4.1 utiliza tácticas engañosas, como el escaneo falso del sistema y mensajes de alerta, para incitar a las víctimas a instalar un controlador supuestamente actualizado, desencadenando así la infección. La nueva variante muestra mejoras significativas en comparación con métodos anteriores y utiliza polimorfia de código avanzada, lo que plantea preocupaciones sobre su capacidad para evadir la detección de antivirus y su impacto potencial en los usuarios.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hackread.com/fake-fix-chaes-4-1-malware-hides-driver-downloads/?web_view=true

---

Hackers utilizan paquetes NPM maliciosos en GitHub para robar claves SSH

Se descubrieron dos paquetes NPM maliciosos, warbeast2000 y kodiak2k, que aprovechan GitHub para almacenar claves SSH robadas en formato Base64 de sistemas de desarrolladores que instalaron los paquetes. Ambos fueron eliminados de NPM en enero. Los paquetes ejecutaban scripts que leían las claves privadas SSH y las subían a un repositorio de GitHub controlado por los atacantes. Este método de alojar infraestructura de control y comando maliciosa en GitHub es parte de una tendencia creciente. Se observa un aumento alarmante en la cantidad de paquetes maliciosos en administradores de paquetes de código abierto. Se recomienda a los desarrolladores

y organizaciones evaluar la seguridad de los paquetes antes de incorporarlos para garantizar su seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/malicious-npm-ssh-key/

Cuidado con las aplicaciones piratas de MacOS que instalan malware

Se descubrió un nuevo malware incrustado en aplicaciones piratas de MacOS, similar al malware ZuRu, que descarga y ejecuta varios payloads para comprometer dispositivos en segundo plano. Estas aplicaciones están alojadas en sitios web piratas chinos para atraer a más víctimas. El malware se dirige específicamente a aplicaciones descargadas ilegalmente, como FinalShell, Microsoft Remote Desktop Client, Navicat Premium, SecureCRT y UltraEdit. Al detonarse, descarga y ejecuta múltiples payloads en segundo plano para comprometer secretamente la máquina de la víctima. Se destaca la importancia de comprender los riesgos asociados con el uso de software pirata y se recomienda a los usuarios utilizar aplicaciones de MacOS que identifiquen y filtren riesgos, además de bloquear el acceso a sitios web conocidos por alojar software pirateado.

Prioridad: 3 Importante.

Ampliar información:

- hhttps://gbhackers.com/beware-of-pirated-macos-apps/

Amenazas financieras emergentes: ataques a bancos y criptomonedas en México

El equipo de investigación de BlackBerry ha identificado un actor financiero que apunta a bancos mexicanos y plataformas de criptomonedas. Utilizando una versión modificada de AllaKore RAT, el

atacante despliega instaladores personalizados, camuflados con esquemas del Instituto Mexicano del Seguro Social. El payload adaptado de AllaKore RAT facilita el robo de credenciales bancarias, enviándolas a un servidor de comando y control. Aunque el enfoque no parece limitarse a una industria específica, las grandes empresas con ingresos superiores a $100 millones son el blanco principal. Se sospecha que el actor opera en América Latina, evidenciado por el uso de direcciones IP de Starlink en México y las instrucciones en español integradas en el malware. Este informe detalla los aspectos técnicos y los indicadores clave asociados con estos ataques persistentes desde finales de 2021.

Prioridad: 2 Urgente.

Ampliar información:

- https://blogs.blackberry.com/en/2024/01/mexican-banks-and-cryptocurrency-platforms-targeted-with-allakore-rat?&web_view=true

---

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

HP Enterprise hackeada por ciberataque ruso relacionado con brecha en DNC

Hewlett Packard Enterprise (HPE), la gigante tecnológica, ha sido víctima de un ciberataque presuntamente llevado a cabo por hackers vinculados al Kremlin. El grupo APT29, también conocido como BlueBravo o Cozy Bear, habría infiltrado el entorno de correo electrónico en la nube de HPE, exfiltrando datos de buzones a partir de mayo de 2023. Aunque HPE descubrió la intrusión en diciembre de 2023, los actores de amenazas estuvieron no detectados durante más de seis meses. Este grupo ha sido previamente asociado con ataques de alto perfil, incluida la brecha del Comité Nacional Demócrata (DNC) en 2016 y la comprometida cadena de suministro de SolarWinds en 2020. El incidente no ha tenido un impacto material en las operaciones de HPE hasta la fecha.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/tech-giant-hp-enterprise-hacked-by.html?&web_view=true

---

VexTrio: la plataforma de delitos cibernéticos que facilita el malware para más de 60 afiliados

El grupo detrás de ClearFake, SocGholish y otros actores ha establecido asociaciones con VexTrio, una entidad que opera como una "plataforma criminal de afiliados". Infoblox revela que VexTrio, activo desde al menos 2017, dirige una red de más de 70,000 dominios, ofreciendo servicios a más de 60 afiliados, incluyendo ClearFake y SocGholish. La compleja red de VexTrio utiliza servidores dedicados para cada afiliado y controla múltiples sistemas de distribución de tráfico para maximizar las ganancias y filtrar contenido no deseado. Su modelo de negocio avanzado lo

convierte en una entidad difícil de clasificar y destruir, actuando como el "capo de las afiliaciones del cibercrimen".

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2024/01/vextrio-uber-of-cybercrime-brokering.html?&web_view=true

---

Vulnerabilidad en la API de Trello expone direcciones de correo electrónico de 15 millones de usuarios

Una brecha en la API de Trello ha llevado a la revelación de direcciones de correo electrónico vinculadas a 15 millones de cuentas. Aprovechando la exposición, se crearon perfiles de datos que combinaban información pública y privada. Aunque la mayoría de los datos filtrados eran públicos, las direcciones de correo deberían haber permanecido privadas. La falla se originó en una API expuesta que permitía la vinculación de correos electrónicos con cuentas de Trello. Trello ha respondido ajustando la API para exigir autenticación en ciertas solicitudes.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/trello-api-abused-to-link-email-addresses-to-15-million-accounts/?&web_view=true

---

Nuevo método para protegerse contra la toma de cuentas móviles

Investigadores de ciencias de la computación han desarrollado un nuevo método para identificar debilidades de seguridad que dejan a las personas vulnerables a ataques de toma de cuentas, donde un atacante obtiene acceso no autorizado a cuentas en línea. El enfoque utiliza lógica formal

para modelar cómo cambia el acceso a la cuenta cuando dispositivos, tarjetas SIM o aplicaciones se desconectan del ecosistema de la cuenta. Los fabricantes de dispositivos y desarrolladores de aplicaciones podrían adoptar este enfoque para catalogar vulnerabilidades y comprender mejor los ataques de hacking complejos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2024/01/22/safeguard-against-mobile-account-takeovers/?web_view=true

---

De megabits a terabits: Gcore Radar advierte sobre una nueva era de ataques DDoS

Gcore ha publicado su último informe Gcore Radar, un informe semestral en el que la empresa comparte análisis internos para rastrear los ataques DDoS. Los hallazgos clave muestran un aumento alarmante en la escala y sofisticación de las amenazas cibernéticas. Se destaca un aumento del 100% anual en el volumen pico de ataques DDoS, alcanzando 1,6 Tbps en la segunda mitad de 2023. Además, se observa una variación en la duración de los ataques, con ataques UDP floods dominando con un 62%. Los Estados Unidos encabezan la lista de fuentes globales de ataques, y las industrias más afectadas son los juegos, el sector financiero y las telecomunicaciones. El informe subraya la necesidad de estrategias de defensa multifacéticas y destaca la importancia de la cooperación internacional para combatir el cibercrimen.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/from-megabits-to-terabits-gcore-radar.html

---