GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4023

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	5	1	
MALWARE	1	4	
NOTICIAS DE CIBERSEGURIDAD	1	1	2

VULNERABILIDADES

Vulnerabilidad Crítica en Cisco IOS XE Bajo Activa Explotación

Cisco emite una advertencia sobre una vulnerabilidad crítica sin parche en su sistema IOS XE que permite a los atacantes obtener control total del dispositivo. Se recomienda desactivar la función del servidor HTTPS de inmediato para protegerse. Un atacante desconocido ya ha explotado esta vulnerabilidad, creando cuentas con privilegios de administrador. Las cuentas persisten incluso después de reiniciar el mismo. Cisco insta a las organizaciones a seguir las pautas de seguridad proporcionadas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/vulnerabilities-threats/critical-unpatched-cisco-zero-day-bug-active-exploit

---

Vulnerabilidad Crítica en Atlassian Confluence

Microsoft ha observado la explotación de una grave vulnerabilidad en Atlassian Confluence Data Center y Server por parte de un actor estatal conocido como Storm-0062. La vulnerabilidad CVE-2023-22515 permite a los atacantes crear cuentas de administrador no autorizadas y acceder a servidores de Confluence. Se recomienda actualizar a las últimas versiones para mitigar amenazas y mantener las aplicaciones aisladas de Internet público hasta que se realicen las correcciones.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/10/microsoft-warns-of-nation-state-hackers.html

---

Vulnerabilidad 'DirtyNIB' en MacOS permite la ejecución de código malicioso

Un investigador de seguridad ha descubierto una nueva vulnerabilidad de día cero en los sistemas MacOS de Apple que permite a los actores de amenazas ejecutar código en nombre de una aplicación legítima de Apple. Aunque Apple ha asignado un CVE con una severidad media a la vulnerabilidad, el investigador sostiene que el problema aún persiste en MacOS y requiere una solución adecuada. La vulnerabilidad se aprovecha mediante la manipulación de archivos NIB, y el informe del investigador detalla cómo se explota esta falla.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/macos-dirtynib-vulnerability/

Exploit en Microsoft Kernel Streaming Server: Casi un Día Cero

Vulnerabilidad tipo día cero en el Microsoft Kernel Streaming Server, que permite a un atacante local aumentar sus privilegios en el sistema. Esta vulnerabilidad, conocida como CVE-2023-36802, fue parcheada por Microsoft el mes pasado. Se detalla el proceso de investigación y explotación de esta vulnerabilidad, destacando la importancia de no dar por sentado las comprobaciones de seguridad en el código. También subraya la necesidad de investigar más a fondo estas vulnerabilidades, ya que podrían ser más comunes de lo que se piensa y presentar riesgos significativos en los controladores de kernel que gestionan la comunicación entre procesos.

Prioridad: 1 Crítico.

Ampliar información:

- https://securityintelligence.com/x-force/critically-close-to-zero-day-exploiting-microsoft-kernel-streaming-service/

Google lanza Chrome 118 con 20 parches, incluyendo uno crítico en Site Isolation

Google ha lanzado Chrome 118 con parches para 20 vulnerabilidades, incluyendo una de gravedad crítica en Site Isolation, una característica de seguridad de Chrome que previene el robo de datos entre sitios web. Aunque no se proporcionan detalles específicos sobre la vulnerabilidad crítica, se trata de un problema de uso después de liberar que podría permitir a los atacantes escapar de las protecciones de seguridad de Chrome. Además de la vulnerabilidad, se han solucionado ocho problemas de gravedad media y cinco de baja gravedad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/chrome-118-patches-20-vulnerabilities/

Vulnerabilidades sin parches exponen los routers industriales de Yifan a ataques

Los routers industriales fabricados por la empresa china Yifan presentan varias vulnerabilidades críticas que pueden exponer a las organizaciones a ataques, según informó el grupo de investigación y amenazas de Cisco, Talos. Aunque se notificó al proveedor en junio y se le dio más de 90 días para lanzar parches, no parece que se hayan publicado correcciones, por lo que Cisco ha hecho públicos los detalles técnicos de acuerdo con su política de divulgación de vulnerabilidades. Estas vulnerabilidades pueden permitir la ejecución de comandos arbitrarios y el acceso no autorizado a los dispositivos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/unpatched-vulnerabilities-expose-yifan-industrial-routers-to-attacks/

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

Paquete Malicioso en NuGet para Desarrolladores .NET con SeroXen RAT

Se ha descubierto un paquete malicioso en el administrador de paquetes NuGet para el Framework .NET que distribuye un troyano de acceso remoto llamado SeroXen RAT. El paquete malicioso es una variante engañosa de un paquete legítimo y ha inflado artificialmente sus descargas. Los atacantes aprovechan scripts para ejecutar código malicioso. Los desarrolladores deben verificar cuidadosamente la autenticidad de los paquetes antes de su instalación.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/10/malicious-nuget-package-targeting-net.html

---

Malware DarkGate se Propaga a través de Servicios de Mensajería

El malware DarkGate se está propagando a través de aplicaciones de mensajería como Skype y Microsoft Teams. Los atacantes utilizan un script VBA disfrazado de PDF para engañar a los usuarios y descargar el malware. Esta táctica se ha utilizado en campañas de ingeniería social, a su vez, la infección ha aumentado en los últimos meses. DarkGate es un malware versátil que puede robar datos, realizar minería de criptomonedas y permitir a los atacantes controlar sistemas de forma remota. La propagación a través de aplicaciones de mensajería representa una amenaza significativa para los usuarios de estas plataformas.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/10/darkgate-malware-spreading-via.html

---

SpyNote: El Peligroso Troyano Android que Graba Llamadas y Audio

El troyano SpyNote para Android es una amenaza que se propaga a través de mensajes SMS engañosos camuflándose en los dispositivos, registrando llamadas, audio y otros datos sensibles. Es extremadamente difícil de eliminar, lo cual, obliga a los usuarios a realizar un restablecimiento de fábrica para deshacerse de él. Los usuarios deben tener cuidado con las aplicaciones no verificadas y los enlaces sospechosos para evitar ser víctimas de este tipo de malware.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/10/spynote-beware-of-this-android-trojan.html

---

Backdoor en Sitios de WordPress Se Hace Pasar por Complemento Legítimo

Un backdoor de WordPress se ha descubierto en sitios web comprometidos, su astucia radica en ocultar su verdadera naturaleza haciéndose pasar por un complemento legítimo. Este malware, que se presenta como un complemento de almacenamiento en caché, se ejecuta en el contexto de WordPress y proporciona a los atacantes una serie de capacidades maliciosas, como la creación de cuentas de administrador o la capacidad de servir contenido malicioso según filtros específicos. Su detección se ha producido durante la limpieza de sitios comprometidos, lo que resalta la importancia de mantener la seguridad en las plataformas de WordPress.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/backdoor-malware-found-on-wordpress-website-disguised-as-legitimate-plugin/

Campaña de Malware DarkGate Abusa de Skype y Teams

Los ciberdelincuentes han aprovechado plataformas de mensajería como Skype y Teams para distribuir el malware DarkGate. Por ello, es importante mantener la seguridad en aplicaciones de mensajería y examinar cuidadosamente cualquier nueva aplicación introducida en una organización para evitar un aumento en la superficie de ataque. El malware DarkGate es una amenaza versátil capaz de realizar diversas operaciones maliciosas, las cuentas comprometidas en aplicaciones de mensajería se utilizan para engañar a las víctimas y ejecutar scripts maliciosos.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/152513/cyber-crime/darkgate-campaign-messaging-platforms.html

---

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

Las 10 configuraciones erróneas más comunes en empresas según NSA y CISA

La Agencia de Seguridad Nacional (NSA) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) han revelado las configuraciones de ciberseguridad más comunes que ponen en riesgo a grandes organizaciones. Estos errores incluyen configuraciones predeterminadas de software, falta de segmentación de red y mal manejo de parches. La NSA y CISA enfatizan la necesidad de que los fabricantes de software adopten principios de seguridad desde el diseño. Se insta a implementar medidas de mitigación, como la eliminación de contraseñas predeterminadas y la autenticación multifactor, para reducir el riesgo de explotación de estas configuraciones erróneas comunes. Las agencias también recomiendan pruebas y validaciones de seguridad contra amenazas conocidas.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2023/10/top-10-de-errores-de-configuracion-en.html

---

Air Europa Insta a Clientes a Cancelar Tarjetas de Crédito Tras Ciberataque

Air Europa ha sufrido un ciberataque en el proceso de reserva de vuelos que resultó en la interceptación de datos financieros de sus clientes. La aerolínea ha notificado a los afectados que los datos de sus tarjetas de crédito, incluyendo número, CVV y fecha de caducidad, fueron robados y les insta a cancelar sus tarjetas. La compañía asegura que los atacantes no accedieron a otras

bases de datos de la aerolínea ni a información personal de los clientes. El ataque ha estado dirigido al entorno de pagos en la web, y la brecha ha sido cerrada. Se espera que el impacto de la filtración se conozca en los próximos días. Esta no es la primera vez que Air Europa enfrenta un ciberataque de esta gravedad; en 2018, medio millón de sus clientes sufrió una brecha similar.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/10/air-europa-pide-sus-clientes-que.html

---

Nuevo Conjunto de Herramientas de ToddyCat para Exfiltración de Datos

El grupo de amenaza persistente avanzada (APT) conocido como ToddyCat ha sido vinculado a un nuevo conjunto de herramientas maliciosas diseñadas para la exfiltración de datos. Estos hallazgos provienen de Kaspersky, que ha estado rastreando al grupo desde el año pasado. Además de sus herramientas previamente identificadas, como Ninja Trojan y Samurai, se han descubierto nuevas herramientas utilizadas para mantener la persistencia, realizar operaciones de archivos y cargar cargas adicionales en tiempo de ejecución. Estas herramientas incluyen cargadores, un recolector de archivos, un cargador de Dropbox y un exfiltrador de archivos. ToddyCat ha estado llevando a cabo actividades de espionaje dirigidas a entidades de alto perfil en Europa y Asia durante varios años, utilizando múltiples técnicas y herramientas sofisticadas.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/10/researchers-unveil-toddycats-new-set-of.html

---

Shufflecake: Sistema Oculto de Almacenamiento de Datos en Linux

Elia Anzuoni y Tommaso Gagliardoni han desarrollado "Shufflecake", una técnica sigilosa para ocultar datos en sistemas Linux, heredera de TrueCrypt y VeraCrypt. Esta técnica opera en el nivel de

bloque del sistema de archivos, permitiendo ocultar datos cruciales y negar su existencia incluso ante adversarios violentos. Shufflecake mejora la seguridad y es de código abierto, promoviendo la confianza y contribuciones de la comunidad.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/shufflecake-linux-filesystems/