GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3823

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	4	1	
MALWARE	1	3	1
NOTICIAS DE CIBERSEGURIDAD	2	1	1

VULNERABILIDADES

Cisco Advierte sobre Intentos de Explotación de Vulnerabilidad Zero-Day en su Software IOS

Cisco ha emitido una advertencia sobre una vulnerabilidad de gravedad media, identificada como CVE-2023-20109, en la función de Grupo de VPN de Transporte Encriptado (GET VPN) de su software IOS e IOS XE, que ha sido objeto de intentos de explotación. La falla podría permitir la ejecución remota de código si un atacante posee credenciales válidas y control administrativo sobre un miembro del grupo o un servidor de claves. Cisco aconseja a todos los clientes que actualicen a una versión parcheada de IOS o IOS XE para abordar esta amenaza potencial.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/cisco-warns-of-ios-software-zero-day-exploitation-attempts/

Google Parchea una Nueva Vulnerabilidad Zero-Day en Chrome

Google ha lanzado una actualización para parchear una nueva vulnerabilidad zero-day en Chrome que estaba siendo explotada por un proveedor de spyware comercial. La vulnerabilidad, identificada como CVE-2023-5217, se trata de un desbordamiento de búfer en la codificación vp8 en libvpx. Fue reportada al equipo de Chrome por Clement Lecigne del Grupo de Análisis de Amenazas (TAG) de Google, apenas dos días antes de que se lanzara el parche. Google advierte que esta vulnerabilidad ya ha sido explotada en la naturaleza y un investigador de TAG reveló que fue utilizada por un proveedor comercial de vigilancia. Esta es la sexta vulnerabilidad zero-day de Chrome que Google ha parcheado en 2023, la actualización también aborda otras vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/google-rushes-to-patch-new-zero-day-exploited-by-spyware-vendor/

Firefox Actualización Crucial para Corregir Vulnerabilidades de Alta Severidad

Firefox 118 ha sido lanzado con la corrección de seis vulnerabilidades de alta severidad, incluyendo problemas de memoria que podrían resultar en bloqueos explotables. Estas vulnerabilidades afectan componentes críticos del navegador y podrían permitir a los atacantes ejecutar código malicioso si se explotan con éxito. Mozilla insta a los usuarios a actualizar a la última versión para mantenerse protegidos contra posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/firefox-118-patches-high-severity-vulnerabilities/

Vulnerabilidades Críticas en Cisco WAN Manager Permiten Ataques DoS

Cisco ha emitido una advertencia crítica de seguridad debido a varias vulnerabilidades en su Catalyst SD-WAN Manager, que podrían permitir el acceso no autorizado y causar una negación de servicio. No existen soluciones temporales disponibles, por lo que se requiere una acción inmediata. Las vulnerabilidades afectan a diversos aspectos del sistema y tienen diferentes grados de gravedad, desde críticas hasta moderadas. Cisco ha lanzado actualizaciones de software para abordar estos problemas y los usuarios con contratos de servicio deben obtener las correcciones correspondientes.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/cisco-wan-manager-vulnerabilities/

Vulnerabilidades Críticas en SharePoint Permiten la Ejecución Remota de Código

Investigadores han revelado una peligrosa cadena de exploits que aprovecha dos vulnerabilidades críticas en Microsoft SharePoint Server. Una de ellas permite la elevación de privilegios y la otra la ejecución de código remoto. Estas vulnerabilidades, aunque ya parcheadas, presentan un alto riesgo, ya que los atacantes podrían obtener acceso no autorizado y controlar servidores de SharePoint. Se estima que más de 100,000 servidores de SharePoint en Internet podrían verse afectados. Los investigadores también han publicado código de prueba de concepto que muestra cómo se podrían aprovechar estas vulnerabilidades, lo que aumenta la preocupación por la seguridad de los sistemas de SharePoint no actualizados.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/vulnerabilities-threats/reseachers-release-details-of-new-rce-exploit-chain-for-sharepoint

---

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

Peligroso Malware Xenomorph: Nueva Campaña de ataque

El malware Xenomorph ha resurgido después de meses de inactividad, expandiendo su lista de objetivos en una nueva campaña que afecta a usuarios de Android en Estados Unidos, España, Portugal, Italia, Canadá y Bélgica. Esta amenaza, que se originó en la tienda oficial de Google Play en

febrero de 2022, se ha desarrollado considerablemente y ahora apunta a más de 400 bancos e instituciones financieras, además de presentar un avanzado motor de automatización que le permite realizar una amplia gama de actividades maliciosas sin interacción humana.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/151443/malware/xenomorph-malware-is-back.html

---

Spyware Predator Explota Vulnerabilidades en iOS y Chrome

Google ha revelado que el spyware Predator se ha aprovechado de vulnerabilidades de día cero en iOS y Chrome, afectando a dispositivos iOS anteriores a la versión 16.7. El ataque se realizó mediante un ataque de intermediario (MitM), redirigiendo a las víctimas a sitios web maliciosos que entregaban el spyware. También se ha observado una cadena de exploits dirigida a dispositivos Android en Egipto. Google no ha identificado todas las vulnerabilidades involucradas en esta cadena, pero confirmó que aprovechaba la vulnerabilidad CVE-2023-4762 para la ejecución remota de código.

Prioridad: 2 Urgente.

Ampliar información:

- hhttps://www.securityweek.com/predator-spyware-delivered-to-ios-android-devices-via-zero-days-mitm-attacks/

Troyano Lu0Bot en Node.js Toma Control Completo de las Computadoras de las Víctimas

Los investigadores de ciberseguridad han descubierto un malware llamado Lu0Bot basado en Node.js que tiene la capacidad de tomar el control completo del sistema de la víctima. Este malware utiliza técnicas de ofuscación y cifrado para evitar la detección y se ha vuelto más complejo en su

diseño. Aunque su actividad ha sido limitada, su capacidad para grabar pulsaciones de teclas, robar identidades y realizar ataques DDoS lo convierte en una amenaza potencialmente peligrosa si su campaña se expande.

Prioridad: 1 Critico.

Ampliar información:

- https://gbhackers.com/lu0bot-node-js-malware/

Ransomware en Auge: Amenazas que Aprovechan Herramientas de Gestión Remota

Los actores de amenazas están utilizando cada vez más herramientas de Gestión y Monitoreo Remoto (RMM) para desplegar ransomware. En una campaña de distribución de ransomware Hive, los atacantes utilizaron un archivo ejecutable disfrazado de documento legítimo como carga original. Esta campaña probablemente se distribuyó por correo electrónico, con un enlace que, al hacer clic en él, descargaba el ejecutable. Se requirió que el usuario final fuera un Administrador local para el método de acceso inicial, ya que los usuarios con privilegios más bajos causarían que la instalación fallara. Los atacantes realizaron una serie de acciones, incluyendo el despliegue de un beacon Cobalt Strike y la ejecución de ransomware Hive en servidores importantes, todo utilizando herramientas y servicios remotos.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/threat-actors-deploy-ransomware/

EvilBamboo Amplía sus Ataques a Dispositivos Android y iOS con Malware Personalizado

El grupo de amenaza EvilBamboo, que antes se centraba en atacar dispositivos iOS, ha ampliado su alcance para dirigirse a usuarios de Android. Utilizando sitios web falsos y perfiles de redes sociales, se hacen pasar por comunidades populares. Su malware incluye tres familias: BADBAZAAR, BADSIGNAL y BADSOLAR, cada una con un backdoor incrustado. Estas aplicaciones maliciosas se distribuyen a través de grupos de Telegram y tienen diversas funcionalidades, desde el robo de SMS hasta la recopilación de información del dispositivo.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/evilbamboo-attacking-android-ios/

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

Hackers del gobierno chino atrapados escondidos en el firmware enrutadores Cisco

El grupo de ciberataque chino BlackTech, respaldado por el gobierno, ha sido detectado utilizando firmware implantado en routers Cisco para mantenerse oculto mientras se desplaza silenciosamente por las redes corporativas de empresas multinacionales en Estados Unidos y Japón. Este ataque ha sido descubierto por la NSA, el FBI, la CISA y el NISC de Japón, que han emitido una advertencia conjunta. Los atacantes modifican el firmware de routers Cisco para ocultar su actividad y mantener la persistencia en la red, lo que les permite moverse de subsidiarias internacionales a las sedes en Japón y Estados Unidos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/chinese-gov-hackers-caught-hiding-in-cisco-router-firmware/

Exposición de Datos de Tesla y Riesgos de Seguridad

Las instancias mal configuradas de TeslaMate pueden exponer información crítica sobre automóviles Tesla y sus propietarios en Internet, permitiendo a posibles atacantes acceder a datos sensibles, como la ubicación en tiempo real del vehículo y la presencia del conductor. Este riesgo surge cuando los usuarios no configuran adecuadamente esta aplicación de terceros, lo que puede llevar a violaciones de privacidad y otros peligros relacionados con la seguridad de los vehículos. La

firma de seguridad IoT Redinent ha identificado más de 1,400 instancias de TeslaMate mal configuradas que permiten un acceso no autorizado.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/misconfigured-teslamate-instances-put-tesla-car-owners-at-risk/

Nuevo Ataque de Canal Lateral GPU.zip Pone en Peligro la Seguridad de las GPUs Modernas

Un grupo de investigadores ha descubierto una nueva forma de ataque de canal lateral llamada "GPU.zip" que afecta a la mayoría de las unidades de procesamiento gráfico (GPU) modernas, incluyendo AMD, Apple, Arm, Intel, Nvidia y Qualcomm. Este ataque se aprovecha de la compresión de datos gráficos basada en hardware, una optimización en las GPU modernas para mejorar el rendimiento. Lo preocupante es que GPU.zip puede ser explotado por sitios web maliciosos, lo que significa que los atacantes pueden robar información de otros sitios web visitados por la víctima al mismo tiempo. Aunque el robo de datos es posible, lleva un tiempo significativo y requiere que el sitio web víctima no esté configurado adecuadamente para prevenir este tipo de fuga de información.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/new-gpu-side-channel-attack-allows-malicious-websites-to-steal-data/

Hackers Utilizan Manipulación del Tamaño de Fuente para Evitar la Seguridad de Office 365

Se ha identificado una nueva técnica de phishing llamada "ZeroFont Phishing", que permite a los ciberdelincuentes eludir las medidas de seguridad de Office 365. A través de esta técnica, los atacantes pueden burlar el procesamiento de lenguaje natural de Microsoft, utilizado para proteger a los usuarios de Office contra correos electrónicos de phishing. Esta técnica involucra la inserción de texto en un correo electrónico con un tamaño de fuente cero, lo que confunde el procesamiento de lenguaje natural y permite que el correo sea entregado a la bandeja de entrada del usuario, a pesar de ser un intento de phishing. Microsoft había estado utilizando este enfoque para detectar señales de suplantación o fraude en el contenido de los correos electrónicos. Sin embargo, los ciberdelincuentes han encontrado una forma de eludir esta protección.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.pandasecurity.com/es/mediacenter/seguridad/usos-inteligencia-artificial-ciberseguridad/