GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2024

En alianza con

TD SYNNEX FORTINET

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	0	4	2
MALWARE	0	1	5
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Tráfico DNS puede filtrarse fuera del túnel VPN en Android

Probablemente hay múltiples fugas de DNS en dispositivos Android. Estas fugas se originan en fallos del propio sistema operativo y solo afectan a ciertas aplicaciones. El lunes 22 de abril se recibió un informe de un usuario en Reddit sobre una fuga de DNS. El informe detallaba cómo el usuario logró filtrar consultas DNS al desactivar y luego activar la VPN mientras la opción "Bloquear conexiones sin VPN" estaba activada. Inmediatamente iniciamos una investigación interna para confirmar el problema. Esta investigación también reveló más situaciones en las que pueden ocurrir fugas de DNS en dispositivos Android.

Prioridad: 3 Importante.

Ampliar información:

https://mullvad.net/en/blog/dns-traffic-can-leak-outside-the-vpn-tunnel-on-android.

Talos revela múltiples vulnerabilidades de día cero

El equipo de investigación de vulnerabilidades de Cisco Talos reveló recientemente tres vulnerabilidades de día cero que aún no han sido parcheadas a partir del miércoles 8 de mayo. Dos de las vulnerabilidades de este grupo, una en el demonio proxy HTTP Tinyroxy y otra en la biblioteca de archivos stb_vorbis.c, podrían llevar a la ejecución arbitraria de código, obteniendo ambas problemas una puntuación CVSS de 9.8 sobre 10. Aunque no pudimos contactar a los mantenedores, los mantenedores de Tinyroxy han parcheado el problema desde entonces. Otro día cero existe en el enrutador inalámbrico Milesight UR32L.

Prioridad: 3 Importante.

Ampliar información:

https://blog.talosintelligence.com/vulnerability-roundup-zero-days-may-8-2024

Citrix advierte a los administradores que mitiguen manualmente el error del cliente SSH PuTTY

Esta semana, Citrix notificó a sus clientes que mitiguen manualmente una vulnerabilidad en el cliente SSH PuTTY que podría permitir a los atacantes robar la clave privada SSH de un administrador de XenCenter. XenCenter ayuda a gestionar los entornos de Citrix Hypervisor desde un escritorio de Windows, incluyendo la implementación y monitorización de máquinas virtuales.

Prioridad: 2 Urgente.

Ampliar información:

https://support.citrix.com/article/CTX633416/citrix-hypervisor-security-update-for-cve202431497

Google corrige el quinto día cero de Chrome explotado en ataques este año

Google ha lanzado una actualización de seguridad para el navegador Chrome para solucionar el quinto día cero explotado en la naturaleza desde el inicio del año. El problema de alta gravedad, identificado como CVE-2024-4671, es una vulnerabilidad de "user after free" en el componente Visuals que maneja el renderizado y la visualización de contenido en el navegador.

Prioridad: 2 Urgente.

Ampliar información:

https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-vulnerability-exploited-in-attacks-in-2024/

Falla crítica en Tinyproxy abre más de 50,000 hosts a la ejecución remota de código

Una vulnerabilidad en Tinyproxy, identificada como CVE-2023-49606, ha sido descubierta por el equipo de investigación de Cisco Talos. Esta falla, con una puntuación CVSS de 9.8 sobre 10, se trata de un error de uso después de liberar memoria que afecta a las versiones 1.10.0 y 1.11.1 del software, siendo esta última la versión más reciente.

Según el informe de Talos, un encabezado HTTP especialmente diseñado puede desencadenar la reutilización de memoria previamente liberada, lo que resulta en corrupción de memoria y podría permitir la ejecución remota de código. Es importante destacar que un atacante solo necesita realizar una solicitud HTTP no autenticada para explotar esta vulnerabilidad.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/05/critical-tinyproxy-flaw-opens-over.html

---

Vulnerabilidades críticas en F5 permiten tomar control del dispositivo

Se han identificado dos vulnerabilidades de seguridad en F5 Next Central Manager que podrían ser aprovechadas por un actor malintencionado para obtener el control de los dispositivos y establecer cuentas de administrador ocultas y fraudulentas, lo que les permitiría mantener la persistencia en el sistema.

- CVE-2024-21793 (puntuación CVSS: 7,5): Esta vulnerabilidad de inyección de OData podría permitir que un atacante no autenticado ejecute consultas SQL maliciosas a través de la API de BIG-IP NEXT Central Manager.
- CVE-2024-26026 (puntuación CVSS: 7,5): Se trata de una vulnerabilidad de inyección SQL que también podría permitir a un atacante no autenticado ejecutar consultas SQL maliciosas a través de la API BIG-IP Next Central Manager.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.segu-info.com.ar/2024/05/vulnerabilidades-criticas-en-f5.html?utm_source=SeguInfo&utm_medium=SeguInfo&utm_campaign=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&utm_content=Segu-Info%20-%20Ciberseguridad%20desde%20el%202000&lctg=205608146

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

Actualizaciones de HijackLoader

HijackLoader (también conocido como IDAT Loader) es un cargador de malware detectado por primera vez en 2023 que es capaz de utilizar una variedad de módulos para inyección y ejecución de código. Utiliza una arquitectura modular, una característica que la mayoría de los cargadores no tienen. Investigadores de ThreatLabz analizaron recientemente una nueva muestra de HijackLoader que presenta técnicas de evasión actualizadas.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/hijack-loader-malware-employs-process.html

---

Nuevo spyware persistente para macOS llamado 'Cuckoo' apunta a Macs con arquitecturas Intel y Arm

Investigadores de ciberseguridad han descubierto un nuevo ladrón de información dirigido a sistemas Apple macOS, diseñado para establecer persistencia en los hosts infectados y actuar como spyware. Denominado Cuckoo por Kandji, el malware es un binario Mach-O universal capaz de ejecutarse tanto en Macs basados en Intel como en Arm. El vector exacto de distribución aún no está claro, aunque hay indicios de que el binario se aloja en sitios como dumpmedia[.]com, tunesolo[.]com, fonedog[.]com, tunesfun[.]com y tunefab[.]com, que afirman ofrecer versiones gratuitas o de pago de aplicaciones dedicadas a ripear música de servicios de streamin, convirtiéndola al formato MP3.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/05/new-cuckoo-persistent-macos-spyware.html

---

Hackers del grupo APT42 se hacen pasar por periodistas para recolectar credenciales y acceder a datos en la nube

Se observó que integrantes del grupo de hackers APT42 se hacían pasar por periodistas y organizadores de eventos para construir confianza con sus víctimas a través de una correspondencia continua, para entregar invitaciones a conferencias o documentos legítimos, dijo la compañía. Estos esquemas de ingeniería social permitieron a APT42

recolectar credenciales y usarlas para obtener acceso inicial a entornos en la nube. Posteriormente, el actor de amenazas exfiltró datos de interés estratégico para Irán de manera encubierta, mientras dependía de funciones integradas y herramientas de código abierto para evitar la detección.

Prioridad: 3 importante.

Ampliar información:

https://thehackernews.com/2024/05/apt42-hackers-pose-as-journalists-to.html

---

Botnet Mirai explota vulnerabilidades de Ivanti Connect Secure para la entrega de carga útil maliciosa

Según los hallazgos de Juniper Threat Labs, dos fallas de seguridad recientemente reveladas en dispositivos Ivanti Connect Secure (ICS) están siendo explotadas para desplegar el botnet Mirai. Las vulnerabilidades CVE-2023-46805 y CVE-2024-21887 han sido aprovechadas para entregar la carga útil del botnet. Mientras que CVE-2023-46805 es una falla de bypass de autenticación, CVE-2024-21887 es una vulnerabilidad de inyección de comandos, lo que permite a un atacante encadenar ambas para ejecutar código arbitrario así como tomar el control de las instancias susceptibles.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/04/android-remote-access-trojan-equipped-to-harvest-credentials/

El malware Hijack Loader emplea el proceso de vaciado para eludir el Control de Cuentas de Usuario (UAC) en su última versión

Se ha observado una nueva versión de un cargador de malware llamado Hijack Loader que incorpora un conjunto actualizado de técnicas anti-análisis para pasar desapercibido. 'Estas mejoras tienen como objetivo aumentar la sigilosidad del malware, permitiéndole permanecer indetectado durante períodos más largos de tiempo', dijo el investigador de Zscaler ThreatLabz, Muhammed Irfan V A, en un informe técnico.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/hijack-loader-malware-employs-process.html

---

Un paquete de Python malicioso oculta el marco de comando y control (C2) Sliver en el logotipo falso de la biblioteca de solicitudes

Los investigadores de ciberseguridad han identificado un paquete Python malicioso que pretende ser un derivado de la popular biblioteca requests. Se ha encontrado que oculta una versión en Golang del framework de comando y control (C2) Sliver dentro de una imagen PNG del logotipo del proyecto. El paquete que utiliza esta estratagema, requests-darwin-lite, que ha sido descargada 417 veces antes de ser eliminada del registro del Índice de Paquetes de Python (PyPI).

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/malicious-python-package-hides-sliver.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

El Salvador sufrió una filtración masiva de datos biométricos

Resecurity identificó una filtración de la información personal identificable (PII) de más de cinco millones de ciudadanos de El Salvador en la Dark Web, afectando a más del 80% de la población del país. El actor de amenazas, que utiliza el alias 'CiberinteligenciaSV', publicó el volcado de datos de 144 GB en los foros de Breach, escribiendo que la filtración incluía 5,129,518 fotos de alta definición, cada una etiquetada con el número de identificación del documento (DUI) correspondiente del salvadoreño. Resecurity evalúa que los verdaderos autores intelectuales de esta brecha parecen tener interés en ocultar su participación,

utilizando el espectro de fondo del grupo Guacamaya y sus intermediarios no oficiales para formar una nube de incertidumbre en torno a los verdaderos actores de amenazas y la cadena de ataque que causó la filtración de datos.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/162790/data-breach/el-salvador-massive-leak-biometric-data.html

---

Nueva Ola de Deepfakes Generados por IA

Todos están hablando de deepfakes, pero la mayoría de los medios sintéticos generados por IA que circulan hoy en día parecerán anticuados en comparación con la sofisticación y el volumen de lo que está por venir. Kevin Mandia, CEO de Mandiant en Google Cloud, dice que es probable que en cuestión de meses llegue la próxima generación de deepfakes de audio y video más realistas y convincentes, producidos en masa con tecnología de IA. 'No creo que [el contenido de deepfake] haya sido lo suficientemente bueno todavía', dijo Mandia en una entrevista con Dark Reading.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/threat-intelligence/cybersecurity-in-a-race-to-unmask-a-new-wave-of-ai-borne-deepfakes