GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2724

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	1	1	1
MALWARE	0	0	3
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

RegreSSHion: vulnerabilidad crítica RCE en OpenSSH (CVE-2024-6387)

Se ha descubierto una vulnerabilidad crítica en OpenSSH, un servidor ampliamente utilizado en sistemas Linux. Esta vulnerabilidad, etiquetada como CVE-2024-6387, es una vulnerabilidad de ejecución remota de código sin autenticación (RCE) que permite a los atacantes ejecutar código arbitrario con privilegios de root.

La amenaza de esta vulnerabilidad es alta, ya que, si se explota, un atacante podría tomar el control total del sistema, instalar malware, manipular datos y crear puertas traseras para un acceso persistente.

Esta vulnerabilidad afecta a las versiones de OpenSSH desde la 8.5p1 hasta la 9.8p1. Las versiones anteriores a la 8.5p1 no son vulnerables a esta amenaza debido a un parche para otra vulnerabilidad (CVE-2006-5051).

Prioridad: 1 Crítica.

Ampliar información:

https://cert.europa.eu/publications/security-advisories/2024-066/pdf

https://www.darkreading.com/cloud-security/regresshion-bug-threatens-takeover-of-millions-of-linux-systems

---

Nueva vulnerabilidad en software Cisco NX-OS (CVE-2024-20399)

Se ha identificado una vulnerabilidad zero-day en dispositivos de red Cisco que está siendo explotada activamente por un grupo de actores de amenazas chinos. Esta vulnerabilidad, conocida como CVE-2024-20399, permite a los atacantes ejecutar código arbitrario de manera remota en los dispositivos afectados.

Los productos afectados incluyen varias líneas de productos Cisco, y se recomienda a los administradores aplicar los parches de seguridad proporcionados por Cisco de inmediato. Además, se aconseja configurar medidas de seguridad adicionales como listas de control de acceso (ACLs) y segmentación de red para mitigar el riesgo de explotación mientras se implementan los parches.

Prioridad: 2 Urgente.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/patch-now-cisco-zero-day-chinese-apt

---

Vulnerabilidad crítica de inyección SQL identificado en Fortra FileCatalyst Workflow (CVE-2024-5276)

Se ha descubierto una vulnerabilidad crítica de inyección SQL en la aplicación Fortra FileCatalyst Workflow. Esta vulnerabilidad, identificada como CVE-2024-5276, permite a un atacante modificar los datos de la aplicación. Los impactos probables incluyen la creación de usuarios administrativos y la eliminación o modificación de datos en la base de datos de la aplicación. Esta vulnerabilidad afecta a todas las versiones de FileCatalyst Workflow desde la versión 5.1.6 Build 135 y anteriores.

Para mitigar esta vulnerabilidad, se recomienda actualizar inmediatamente a la versión parcheada (Build 139) para mitigar el riesgo de explotación. Para aquellos que no pueden actualizar de inmediato, deshabilitar el acceso anónimo en el sistema Workflow puede reducir la exposición a posibles ataques que aprovechan CVE-2024-5276.

Prioridad: 3 Importante.

Ampliar información:

https://nvd.nist.gov/vuln/detail/CVE-2024-5276
https://thehackernews.com/2024/06/critical-sqli-vulnerability-found-in.html

---

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

SnailLoad: un nuevo ataque de canal lateral que explota la latencia de la red

Un nuevo ataque de canal lateral llamado SnailLoad ha sido descubierto por un equipo de investigadores de la Universidad Tecnológica de Graz. Este ataque explota la latencia de la red para inferir la actividad del usuario. No requiere JavaScript ni la ejecución de ningún código en el sistema de la víctima, simplemente implica que la víctima cargue contenido de un servidor controlado por el atacante que envía datos a una velocidad extremadamente lenta.

La amenaza de que se materialice esta vulnerabilidad es alta. Si se explota, un atacante podría recopilar información sobre los sitios web visitados o los videos vistos por las víctimas sin necesidad de acceso directo a su tráfico de red.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/new-snailload-attack-exploits-network.html
https://www.snailload.com/

Portal de soporte del fabricante de Routers hackeado, responde con phishing de MetaMask

El portal de soporte de un fabricante de routers, identificado como Mercku, ha sido comprometido. Los investigadores de BleepingComputer han verificado que el portal de ayuda está enviando correos electrónicos de phishing de MetaMask en respuesta a los nuevos tickets de soporte presentados. Este ataque es especialmente preocupante ya que MetaMask, debido a su popularidad, a menudo se convierte en un objetivo para los atacantes, incluyendo actores de phishing y estafadores de criptomonedas. Los clientes y prospectos de Mercku deben abstenerse de usar el portal de soporte del fabricante y de interactuar con cualquier comunicación que provenga de él.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/router-makers-support-portal-hacked-replies-with-metamask-phishing/

Productos de la firma de software india Conceptworld hackeados para propagar malware de robo de datos

Los instaladores de tres diferentes productos de software desarrollados por una empresa india llamada Conceptworld han sido troyanizados para distribuir malware de robo de información. El descubrimiento de este compromiso en la cadena de suministro fue realizado por la firma de ciberseguridad Rapid7. Los instaladores corresponden a Notezilla, RecentX y Copywhiz.

La amenaza de que se materialice esta vulnerabilidad es alta. Si se explota, un atacante podría recopilar información sensible del usuario. Los usuarios de Notezilla, RecentX y Copywhiz están instados a verificar si han sido comprometidos.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/07/indian-software-firms-products-hacked.html
https://vulners.com/thn/THN:4859B3A002CCCF60A5093C0944DC78C7

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

Estafa cibernética: falsa página web de EPM engaña a usuarios para realizar pagos fraudulentos

De acuerdo con un artículo publicado en Semana, se ha identificado una estafa cibernética que involucra a las Empresas Públicas de Medellín (EPM). Los ciberdelincuentes han creado una página web falsa que imita la página oficial de EPM con el objetivo de engañar a los clientes para que realicen pagos a través de esta. La estafa funciona redirigiendo a los clientes a una cuenta bancaria controlada por los atacantes en lugar de la cuenta oficial de EPM. Para proteger a sus clientes, EPM ha compartido una serie de recomendaciones sobre cómo realizar pagos de manera segura y ha enfatizado la importancia de utilizar solo los canales oficiales para realizar transacciones.

Prioridad: 2 Urgente.

Ampliar información:

https://www.semana.com/tecnologia/articulo/asi-estan-estafando-con-falsa-pagina-web-de-epm-senales-para-identificar-el-portal-original/202410/

La mitad de las personas ya no contesta a números desconocidos

Un estudio reciente realizado por Sherlock Communications, reveló que el acoso virtual mediante llamadas y mensajes no deseados, de spam o engañosos ha modificado la manera como las personas en Latinoamérica reaccionan ante este ciberacoso. Según las cifras, más del 50% de los habitantes en la región ya no contestan a números desconocidos debido al alto número de llamadas molestas. Además, un 24% ha perdido llamadas importantes y un 27% ha dejado de leer mensajes de texto. Este panorama ha llevado a

países como Colombia, México, Chile y Costa Rica a reforzar los marcos legales en pro de la protección de datos y el uso responsable de la tecnología y las comunicaciones.

Prioridad: 3 Importante.

Ampliar información:

https://www.eltiempo.com/tecnosfera/novedades-tecnologia/acoso-mediante-llamadas-y-mensajes-en-latinoamerica-la-mitad-de-las-personas-ya-no-contestan-a-desconocidos-3358084

Ticketmaster notifica a los usuarios sobre reciente brecha de datos masiva

Ticketmaster ha comenzado a notificar a los clientes que se vieron afectados por una brecha de datos después de que los hackers robaran la base de datos de Snowflake de la compañía, que contiene los datos de millones de personas. La actividad no autorizada se descubrió en una base de datos en la nube aislada alojada por un proveedor de servicios de datos de terceros. Aunque la cuenta de Ticketmaster permanece segura y los clientes pueden continuar realizando transacciones de manera normal y sin problemas, deben estar alerta.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/ticketmaster-sends-notifications-about-recent-massive-data-breach/
