GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2324

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	2	0	3
MALWARE	0	1	4
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

Vulnerabilidad de Elevación de Privilegios en Windows 10 PlugScheduler

Una vulnerabilidad en Windows 10 permite la escritura arbitraria de archivos como SYSTEM. El componente RUXIM de Windows Update, y específicamente la tarea programada PLUGScheduler, ejecuta operaciones críticas de archivos en un directorio con control parcial por parte de usuarios estándar, lo que podría ser explotado para elevar privilegios.

Prioridad: 1 Crítica.

Ampliar información:

https://www.synacktiv.com/advisories/windows-10-plugscheduler-elevation-of-privilege

Vulnerabilidad CVE-2024-23108 de Inyección de Comandos en Fortinet FortiSIEM

Una vulnerabilidad, identificada como CVE-2024-23108, afecta a las versiones de FortiSIEM 7.1.0 a 7.1.1 y 7.0.0 a 7.0.2 y 6.7.0 a 6.7.8 y 6.6.0 a 6.6.3 y 6.5.0 a 6.5.2 y 6.4.0 a 6.4.2 . Tiene una puntuación CVSS3 de 10.0 y permite la ejecución remota y no autenticada de comandos como root. Estos problemas se encuentran en la forma en que se manejan ciertos parámetros en datastore.py, permitiendo inyección de comandos.

Prioridad: 1 Crítica.

Ampliar información:

https://www.horizon3.ai/attack-research/disclosures/cve-2024-23108-fortinet-fortisiem-2nd-order-command-injection-deep-dive/

Inyección de SQL Basada en el Registro de Auditoria del Servidor Zabbix CVE-2024-22120

Se ha identificado una vulnerabilidad crítica en el servidor Zabbix, identificada como CVE-2024-22120, que permite la ejecución de comandos para scripts configurados. Después de ejecutar un comando, se agrega una entrada de auditoría al "Registro de Auditoría". Debido a que el campo “clientip” no está sanitizado, es posible realizar una inyección SQL en “clientip” y explotar la vulnerabilidad.

Prioridad: 3 Importante.

Ampliar información:

https://support.zabbix.com/browse/ZBX-24505

Vulnerabilidad CVE-2024-1102 que afecta Red Hat Keycloak DBProperties

Se ha identificado una vulnerabilidad en varios productos de Red Hat, como Keycloak, Data Grid y JBoss. Esta vulnerabilidad afecta la función dbProperties y puede conducir a la divulgación de información sensible debido a la manipulación de una entrada desconocida. exponiendo datos confidenciales a actores no autorizados y comprometiendo la confidencialidad.

Prioridad: 3 Importante.

Ampliar información:

https://vuldb.com/?id.262028

Vulnerabilidad en Copilot y Recall que facilita el robo de datos en PCs con Windows

La nueva función de Microsoft, Copilot+ Recall, registra constantemente capturas de pantalla de las PCs de los usuarios, creando una base de datos de su actividad, comparable con una memoria fotográfica. Aunque se exploró su funcionalidad inicial, la reacción de los usuarios fue mayormente negativa, contrastando con su potencial utilidad gerencial para recuperar rápidamente tareas pasadas. Sin embargo, una vulnerabilidad crítica permite a los atacantes robar información personal con solo dos líneas de código, lo que representa un gran riesgo de seguridad.

Prioridad: 3 Importante.

Ampliar información:

https://doublepulsar.com/recall-stealing-everything-youve-ever-typed-or-viewed-on-your-own-windows-pc-is-now-possible-da3e12e9465e

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

Phishing a través de Cloudflare Workers

Netskope Threat Labs está monitoreando varias campañas de phishing que explotan Cloudflare Workers. Estas campañas, que parecen ser obra de diferentes atacantes, emplean dos técnicas distintas. Una de ellas, similar a la campaña Azorult utiliza el código HTML para ocultar el contenido de phishing de la inspección de red.

Prioridad: 3 Importante.

Ampliar información:

https://www.netskope.com/blog/phishing-with-cloudflare-workers-transparent-phishing-and-html-smuggling

---

LilacSquid El Trio sigiloso de PurpleInk, InkBox y InkLoader

Un informe de Talos señala que la campaña "LilacSquid" ha estado activa desde al menos 2021, enfocándose en comprometer organizaciones de diferentes sectores en Asia, Europa y Estados Unidos. Se cree que las actividades de esta campaña están dirigidas por un actor de amenazas persistentes avanzadas (APT) con el objetivo de robar datos y establecer acceso a largo plazo. Las industrias afectadas incluyen farmacéutica, petróleo y gas y tecnología.

Prioridad: 3 importante.

Ampliar información:

https://blog.talosintelligence.com/lilacsquid/

Paquete de NPM que Deja RAT Dirigido a Usuarios de Gulp

Investigadores de ciberseguridad han encontrado un nuevo paquete sospechoso en el registro de paquetes npm, diseñado para instalar un troyano de acceso remoto en sistemas comprometidos. El paquete glup-debugger-log, que se hace pasar por un "registrador para gulp y complementos de gulp", ha sido descargado 175 veces hasta la fecha. La empresa de seguridad Phylum, que descubrió el paquete, ha identificado dos archivos ofuscados que trabajan juntos para desplegar la carga maliciosa.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/06/researchers-uncover-rat-dropping-npm.html

---

Botnet CatDDos y la Técnica de Ataque DDos DNSBomb

Investigadores de Ciberseguridad han identificado una campaña de malware denominada CatDDoS, que ha aprovechado más de 80 vulnerabilidades conocidas en diversos software en los últimos tres meses. Esta campaña utiliza dispositivos vulnerables para formar un botnet y llevar a cabo ataques DDoS. Las vulnerabilidades afectan a una amplia gama de dispositivos y equipos de red de varios proveedores conocidos.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/researchers-warn-of-catddos-botnet-and.html

---

Bancos Brasileños Son Objetivo de una Nueva Variante del RAT AllaKore Llamada AllaSenha

Los bancos brasileños están siendo atacados por una nueva campaña que distribuye una variante personalizada del troyano de acceso remoto AllaKore llamada AllaSenha. Este malware tiene como objetivo robar credenciales de acceso a cuentas bancarias brasileñas y utiliza la infraestructura de Azure cloud como comando y control. Los bancos afectados incluyen a Banco do Brasil, Bradesco, Banco Safra, Caixa Econômica Federal, Itaú Unibanco, Sicoob y Sicredi. Aunque el vector de acceso inicial no está confirmado, se sospecha del uso de enlaces maliciosos en mensajes de phishing.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/05/brazilian-banks-targeted-by-new.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 lado oscuro de Temu

Un informe de Grizzly Research revela que Temu, una popular app conocida por regalar productos y ofrecer grandes descuentos, es un negocio fraudulento. La app recopila datos de los dispositivos de los usuarios para venderlos al mejor postor. Nathan Espinoza, en un video viral de TikTok, explica que Temu es la versión occidental de la plataforma china Pinduoduo, bajo investigación por prácticas similares. PDD Holding Inc., propietaria de Temu, está siendo investigada en Estados Unidos por instalar malware en dispositivos. Las autoridades sospechan que la app obtiene más datos de los permitidos por su política de seguridad.

Prioridad: 3 Importante.

Ampliar información:

https://www.lavanguardia.com/tecnologia/aplicaciones/20230928/9256797/lado-oscuro-temu-app-mas-descargada-espana-comercio-electronico.html?s=08

Ataques Recientes subrayan la crítica necesidad de proteger dispositivos OT externos en Internet

Microsoft ha notado un aumento en los informes de ataques a dispositivos de tecnología operativa (OT) mal protegidos y expuestos en internet. Equipos de OT en sistemas de agua y aguas residuales en Estados Unidos han sido blanco de múltiples ataques en los últimos meses por diferentes actores respaldados por naciones. Estos incidentes resaltan la necesidad urgente de mejorar la seguridad de los dispositivos OT para evitar que los sistemas críticos sean vulnerables a futuros ataques.

Prioridad: 3 Importante.

Ampliar información:

https://www.microsoft.com/en-us/security/blog/2024/05/30/exposed-and-vulnerable-recent-attacks-highlight-critical-need-to-protect-internet-exposed-ot-devices/?s=08

El foro BREACH FORUMS regresó a la dark Web

El foro BREACH FORUMS ha regresado a la dark web, apenas dos semanas después de que el FBI confiscara su infraestructura y arrestara a dos administradores. A pesar de los esfuerzos del FBI, uno de los administradores, ShinyHunters, logró recuperar los dominios, lo que destaca importantes contratiempos operativos y fallas de seguridad en el proceso.

Prioridad: 3 Importante.

Ampliar información:

https://www.theregister.com/2024/05/28/breachforums_back_online/