GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °2124

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

VULNERABILIDADES

Nueva vulnerabilidad de día cero en Chrome CVE-2024-4761 bajo explotación activa

Google lanzó correcciones de emergencia para una nueva vulnerabilidad de día cero en Chrome, identificada como CVE-2024-4761, que está siendo explotada activamente. Esta vulnerabilidad de alta gravedad, un error de escritura fuera de límites en el motor V8 de JavaScript y WebAssembly, fue reportada de manera anónima el 9 de mayo de 2024. Los errores de este tipo pueden ser utilizados por atacantes maliciosos para corromper datos, causar fallos o ejecutar código arbitrario. Google ha reconocido la existencia de un exploit en la naturaleza pero ha retenido detalles específicos para evitar un mayor abuso. Esta corrección se suma a la reciente solución de otra vulnerabilidad, CVE-2024-4671, y eleva a seis el total de vulnerabilidades de día cero solucionadas por Google en lo que va del año.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/new-chrome-zero-day-vulnerability-cve.html

---

Adobe ha solucionado múltiples fallos críticos en Acrobat y Reader

Adobe ha abordado múltiples vulnerabilidades de ejecución de código en sus productos, incluidos Adobe Acrobat y Reader. El gigante del software lanzó sus actualizaciones de Patch Tuesday para solucionar 35 vulnerabilidades de seguridad, 12 de las cuales afectan al software Adobe Acrobat y Reader. Los problemas de ejecución de código arbitrario solucionados incluyen "Use After Free" (uso después de liberación), validación de entrada incorrecta y control de acceso inadecuado. El equipo PSIRT de Adobe no tiene conocimiento de ataques en la naturaleza que exploten estas vulnerabilidades.

Prioridad: 3 Importante.

Ampliar información:

https://securityaffairs.com/163194/security/adobe-flaws-acrobat-reader.html

---

Vulnerabilidad de día cero en Microsoft Windows DWM está lista para una explotación masiva

En la actualización de Patch Tuesday de mayo, Microsoft ha abordado un trío de vulnerabilidades de día cero, destacando un total de 59 CVEs. Una de estas vulnerabilidades, que ya está siendo explotada por los operadores de QakBot, está lista para una explotación masiva. Las fallas reveladas este mes afectan a una amplia gama de productos de Microsoft, incluyendo Windows, Office, .NET Framework, Visual Studio,

Microsoft Dynamics 365, Power BI, DHCP Server, Microsoft Edge (basado en Chromium) y Windows Mobile Broadband. Solo una de estas vulnerabilidades es considerada crítica por Microsoft. Además, el navegador Edge basado en Chromium está afectado por CVE-2024-4761, una vulnerabilidad de día cero en Chrome que Google ya ha parcheado y que permite escapar del sandbox, lo que requiere una corrección inmediata.

Prioridad: 2 Urgente.

Ampliar información:

https://www.darkreading.com/vulnerabilities-threats/microsoft-windows-dwm-zero-day-mass-exploit

---

Nueva vulnerabilidad en WiFi: el ataque de confusión SSID

Una nueva vulnerabilidad derivada de un defecto de diseño en el estándar WiFi permite a los atacantes engañar a las víctimas para que se conecten a redes menos seguras e intercepten su tráfico. Además, el ataque puede explotar la función de desconexión automática en ciertos clientes VPN, que deshabilita automáticamente la conexión VPN cuando el dispositivo se conecta a una red WiFi "confiable" predefinida. Top10VPN se ha asociado con el investigador de seguridad altamente experimentado Mathy Vanhoef para compartir esta vulnerabilidad WiFi antes de su presentación en la conferencia WiSec '24 en Seúl.

Prioridad: 3 Importante.

Ampliar información:

https://www.top10vpn.com/research/wifi-vulnerability-ssid/

Intel ha publicado 41 avisos de seguridad que abordan más de 90 vulnerabilidades

Este Patch Tuesday, Intel ha publicado 41 nuevos avisos de seguridad que cubren un total de más de 90 vulnerabilidades encontradas en los productos de la compañía. El gigante de los chips ha lanzado parches para la mayoría de estas vulnerabilidades, mientras que para algunas ha proporcionado mitigaciones.

Prioridad: 3 Importante.

Ampliar información:

https://www.securityweek.com/intel-publishes-41-security-advisories-for-over-90-vulnerabilities/

Múltiples vulnerabilidades en Fortinet

Se han descubierto vulnerabilidades en varios productos de Fortinet que podrían permitir a un atacante remoto ejecutar código de forma remota, negar el servicio, elevar privilegios y eludir las restricciones de seguridad en el sistema objetivo.

- CVE-2023-36640
- CVE-202345586
- CVE-2024-23664
- CVE-2023-44247
- CVE-2023-46714
- CVE-2024-23665
- CVE-2023-45583
- CVE-2024-23107
- CVE-2024-23667
- CVE-2024-23668
- CVE-2024-23669

- CVE-2024-23670
- CVE-2024-26007
- CVE-2024-31488

Prioridad: 2 Urgente.

Ampliar información:

https://fortiguard.fortinet.com/psirt/FG-IR-24-040

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

El grupo Turla despliega puertas traseras LunarWeb y LunarMail en misiones diplomáticas

Un Ministerio de Asuntos Exteriores (MFA) europeo no identificado y sus tres misiones diplomáticas en el Medio Oriente fueron blanco de dos puertas traseras no documentadas anteriormente, conocidas como LunarWeb y LunarMail. ESET, que identificó la actividad, la atribuyó con confianza media al grupo de ciberespionaje alineado con Rusia Turla (también conocido como Iron Hunter, Pensive Ursa, Secret Blizzard, Snake, Uroburos y Venomous Bear), citando coincidencias tácticas con campañas anteriores identificadas como orquestadas por el grupo. "LunarWeb, desplegado en servidores, utiliza HTTP(S) para sus comunicaciones de C&C [comando y control] y simula solicitudes legítimas, mientras que LunarMail, desplegado en estaciones de trabajo, persiste como un complemento de Outlook y utiliza mensajes de correo electrónico para sus comunicaciones de C&C", dijo el investigador de seguridad Filip Jurčacko.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/05/turla-group-deploys-lunarweb-and.html

---

Compromiso detectado en dispositivos Global Protect de Palo Alto Networks

El mes pasado, Volexity informó sobre su descubrimiento de la explotación de día cero en la naturaleza de CVE-2024-3400 en la función Global Protect de Palo Alto Networks PAN-OS

por parte de un actor de amenazas que Volexity rastrea como UTA0218. Palo Alto Networks publicó un aviso y una firma de protección contra amenazas para la vulnerabilidad dentro de las 48 horas posteriores a la divulgación del problema a Palo Alto Networks por parte de Volexity, con parches y soluciones oficiales que siguieron poco después.

Prioridad: 3 Importante.

Ampliar información:

https://www.volexity.com/blog/2024/05/15/detecting-compromise-of-cve-2024-3400-on-palo-alto-networks-globalprotect-devices/

Los hackers de Kimsuky despliegan una nueva puerta trasera de Linux en ataques contra Corea del Sur

El grupo de hackers norcoreano Kimsuky, ha estado utilizando un nuevo malware de Linux llamado Gomir, que es una versión de la puerta trasera GoBear entregada a través de instaladores de software troyanizados. Kimsuky es un actor de amenazas respaldado por el estado vinculado a la inteligencia militar de Corea del Norte, la Oficina General de Reconocimiento (RGB). A principios de febrero de 2024, investigadores de la empresa de inteligencia de amenazas SW2 informaron sobre una campaña en la que Kimsuky utilizó versiones troyanizadas de varias soluciones de software, como TrustPKI y NX_PRNMAN de SGA Solutions, Wizvera VeraPort, para infectar objetivos surcoreanos con Troll Stealer y el malware de Windows basado en Go, GoBear. Los analistas de Symantec, una empresa de Broadcom, que investigaron la misma campaña dirigida a organizaciones gubernamentales surcoreanas, descubrieron una nueva herramienta maliciosa que parece ser una variante de Linux de la puerta trasera GoBear.

Prioridad: 3 importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/kimsuky-hackers-deploy-new-linux-backdoor-in-attacks-on-south-korea/

Nuevo troyano bancario para Android imita una aplicación de actualización de Google Play

Se ha detectado un nuevo troyano bancario dirigido a dispositivos Android por Cyble Research and Intelligence Labs (CRIL), la rama de investigación del proveedor de inteligencia de amenazas Cyble. En un informe publicado el 16 de mayo, CRIL describió un malware sofisticado que incorpora una variedad de características maliciosas, incluidos ataques de superposición, registro de teclas y capacidades de ofuscación. Los investigadores llamaron al troyano "Antidot" después de una cadena dentro de su código fuente. Antidot se presenta como una aplicación de actualización de Google Play, mostrando una página falsa de actualización de Google Play al ser instalada. Cyble observó que esta falsa página de actualización ha sido elaborada en varios idiomas, incluidos alemán, francés, español, ruso, portugués, rumano e inglés.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/android-banking-trojan-google-play/

Se ha detectado una variante del troyano SugarGh0st RAT utilizada en ataques dirigidos a la industria de la inteligencia artificial (IA)

Investigadores de ciberseguridad han descubierto recientemente una sofisticada campaña cibernética dirigida a organizaciones involucradas en iniciativas de inteligencia artificial en Estados Unidos. La campaña de mayo de 2024, denominada UNK_SweetSpecter, emplea el SugarGh0st RAT, un troyano de acceso remoto adaptado del

Gh0stRAT. Esta variante, históricamente vinculada a actores de amenazas de habla china, ha sido reutilizada ahora para atacar entidades relacionadas con la inteligencia artificial.

Prioridad: 3 Importante.

Ampliar información:

https://www.infosecurity-magazine.com/news/sugargh0st-rat-targeted-ai

---

Campaña de publicidad maliciosa en curso conduce a ransomware

Rapid7 ha observado una campaña en curso para distribuir instaladores troyanizados de WinSCP y PuTTY a través de anuncios maliciosos en motores de búsqueda comúnmente utilizados, donde hacer clic en el anuncio lleva a dominios con errores tipográficos. En al menos un caso observado, la infección ha llevado al intento de despliegue de ransomware. El análisis realizado por Rapid7 presenta actualizaciones a investigaciones pasadas, incluyendo una variedad de nuevos indicadores de compromiso, una regla YARA para ayudar a identificar DLLs maliciosos y algunos cambios observados en la funcionalidad del malware.

Prioridad: 2 Urgente.

Ampliar información:

https://www.rapid7.com/blog/post/2024/05/13/ongoing-malvertising-campaign-leads-to-ransomware/

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

Banco Santander advierte sobre una violación de datos que expuso información de clientes

Banco Santander S.A. anunció que sufrió una violación de datos que afectó a los clientes después de que un actor no autorizado accediera a una base de datos alojada por uno de sus proveedores de servicios externos. Con una fuerte presencia en España, el Reino Unido, Brasil, México y Estados Unidos, Banco Santander es uno de los bancos más grandes y significativos del mundo, conocido por una amplia gama de productos y servicios financieros, que atienden a más de 140 millones de clientes.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/banco-santander-warns-of-a-data-breach-exposing-customer-info

---

FBI confisca foro de piratería BreachForums

El FBI ha confiscado el conocido foro de piratería BreachForums, que filtraba y vendía datos corporativos robados a otros ciberdelincuentes. La confiscación ocurrió el miércoles por la mañana, poco después de que el sitio fuera utilizado la semana pasada para filtrar datos robados de un portal de aplicación de la ley de Europol. El sitio web ahora muestra un mensaje que indica que el FBI ha tomado el control sobre él y los datos de backend, lo que indica que las fuerzas del orden se apoderaron tanto de los servidores como de los dominios del sitio.

Prioridad: 3 Importante.

Ampliar información:

https://www.theregister.com/2024/05/15/fbi_breachforums_ransomware/