GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1624

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

VULNERABILIDADES

Microsoft Outlook RCE CVE-2024-21378 Exploit

La vulnerabilidad CVE-2024-21378, específicamente orientada a MS Outlook, presenta un riesgo significativo en la seguridad informática al permitir la ejecución remota de código malicioso. Para explotar esta vulnerabilidad, se ha diseñado una DLL que se integra con la herramienta Ruler, ampliamente utilizada en pruebas de seguridad. Esta DLL, concebida para comunicarse con Outlook, puede ser utilizada para realizar pruebas de penetración y evaluar la susceptibilidad del sistema a ataques cibernéticos. La colaboración entre la herramienta Ruler y esta DLL acentúa la necesidad de una vigilancia constante y una respuesta rápida por parte de los equipos de seguridad informática para mitigar el riesgo asociado con esta vulnerabilidad.

Prioridad: 1 Crítico.

Ampliar información:

https://system32.ink/microsoft-outlook-rce-cve-2024-21378-exploit/#

Vulnerabilidad en Rust CVE-2024-24576

Se ha identificado una vulnerabilidad crítica en la biblioteca estándar de Rust, anterior a la versión 1.77.2, la cual, afecta específicamente a los sistemas Windows que invocan archivos por lotes ('bat' y 'cmd') utilizando el 'Comando'. Esta vulnerabilidad radica en la falta de escapado adecuado de los argumentos, lo que permite a un atacante ejecutar comandos de shell arbitrarios al controlar los argumentos pasados al proceso generado. La gravedad de esta vulnerabilidad requiere atención inmediata por parte de los usuarios que utilicen archivos por lotes en Windows con argumentos no confiables. Es importante destacar que esta vulnerabilidad no afecta a otras plataformas o usos de Rust.

Prioridad: 2 Urgente.

Ampliar información:

https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-2457

Microsoft corrige 149 fallas

Microsoft ha lanzado su actualización mensual de seguridad para abril de 2024, destinada a abordar un total de 149 fallas de seguridad. Dos de estas vulnerabilidades han sido identificadas como objeto de explotación activa en la naturaleza, lo que subraya la importancia de aplicar los parches de manera urgente. Del total de fallos, tres se clasifican

como críticos, 142 como importantes, tres como moderados y uno como de baja gravedad. Además, la actualización incluye correcciones para 21 vulnerabilidades en el navegador Edge basado en Chromium, que se suman a las actualizaciones anteriores lanzadas en marzo de 2024. Se recomienda a los usuarios y administradores de sistemas aplicar estas actualizaciones lo antes posible para mitigar los riesgos de seguridad.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/microsoft-fixes-149-flaws-in-huge-april.html?m=1

Puerta trasera en XZ que afecta a SSH y Systemd

Un ingeniero de Microsoft identificó una puerta trasera en las utilidades de la versión 5.6 de XZ, un formato de compresión ampliamente utilizado en sistemas Unix y Linux. Esta puerta trasera fue introducida deliberadamente por alguien que se hace llamar Jia Tan, también conocido como JiaT75. El proceso de inserción de esta puerta trasera fue complejo y requirió de astucia por parte del atacante, lo que subraya la importancia de una vigilancia constante en materia de seguridad cibernética. Aunque la detección de la puerta trasera ofrece cierto alivio, este incidente resalta la necesidad de mantener una estricta seguridad en el desarrollo y la distribución de software para proteger contra amenazas.

Prioridad: 2 Urgente.

Ampliar información:

https://www.muylinux.com/2024/04/01/puerta-trasera-xz-ssh-systemd-linux/

Fortinet lanza parches de seguridad críticos para la vulnerabilidad de FortiClientLinux

Fortinet ha respondido de manera proactiva al lanzar parches para abordar una vulnerabilidad crítica en FortiClientLinux, registrada como CVE-2023-45590. Esta vulnerabilidad, con una puntuación CVSS de 9.4 sobre 10, implica un control inadecuado de la generación de código, lo que potencialmente permite la ejecución de código arbitrario. Según Fortinet, un atacante no autenticado podría aprovechar esta vulnerabilidad induciendo a un usuario de FortiClientLinux a visitar un sitio web malicioso. La rápida respuesta de Fortinet subraya su compromiso con la seguridad de sus productos y la protección de sus usuarios contra amenazas cibernéticas. Se recomienda a los usuarios de FortiClientLinux que apliquen los parches proporcionados por Fortinet lo antes posible para mitigar el riesgo asociado con esta vulnerabilidad.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.ehcgroup.io/2024/04/11/10/38/43/16881/fortinet-lanza-parches-de-seguridad-criticos-para-la-vulnerabilidad-de-forticlientlinux/noticias-de-seguridad/ehacking

---

Múltiples vulnerabilidades de ejecución remota de código en JumpServer

El equipo de investigación de amenazas de SonicWall Capture Labs se ha percatado de un par de vulnerabilidades de ejecución remota de código en JumpServer, además, evaluó su impacto, desarrollando medidas de mitigación. JumpServer es un bastión host de código abierto y un sistema de auditoría de seguridad de operaciones, así como mantenimiento profesional con una presencia significativa en la región de China. Un bastión host es una computadora especializada, intencionalmente expuesta en una red pública, diseñada para resistir ataques en una red, nombrada en honor a una fortificación militar.

Prioridad: 3 Importante.

Ampliar información:

https://blog.sonicwall.com/en-us/2024/04/multiple-remote-code-execution-vulnerabilities-in-jumpserver/

Vulnerabilidad en Palo Alto CVE-2024-3400

Palo Alto Networks ha anunciado el descubrimiento de una vulnerabilidad crítica que ha sido explotada, impactando la función GlobalProtect del software PAN-OS. Las correcciones para PAN-OS 10.2, PAN-OS 11.0 y PAN-OS 11.1 están actualmente en desarrollo y se prevé que sean publicadas antes del 14 de abril de 2024.

Versiones afectadas:

- Versión PAN-OS 11.1 anteriores a 11.1.2-h3
- Versión PAN-OS 11.0 anteriores a 11.0.4-h1
- Versión PAN-OS 10.2 anteriores a 10.2.9-h1

Prioridad: 1 Crítico.

Ampliar información:

https://s2grupo.es/vulnerabilidad-critica-en-palo-alto-pan-os/#:~:text=Palo%20Alto%20ha%20publicado%20una,14%20de%20abril%20de%202024

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 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

Ataque a la cadena de suministro de GitHub

Actores maliciosos han lanzado un ataque a la cadena de suministro de software dirigido a desarrolladores en la plataforma GitHub. Barracuda recomienda tomar medidas proactivas detalladas en este aviso de amenaza de ciberseguridad para mitigar el riesgo.

Prioridad: 2 Urgente.

Ampliar información:

https://blog.barracuda.com/2024/05/cybersecurity-threat-advisory-github-supply-chain-attack

---

El último marco de ataque MuddyWater

Durante la "Guerra de Espadas de Hierro" contra los terroristas de Hamas, los actores de amenazas iraníes aumentaron la intensidad de sus operaciones falsas de "hackeo y filtración" dirigidas a empresas israelíes en el sector privado. Esta publicación de blog destaca algunos de los ataques recientes llevados a cabo y proporciona un análisis de "DarkBeatC2", el último marco de comando y control (C2) en el arsenal de MuddyWater.

Prioridad: 3 Importante.

Ampliar información:

https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework

---

La campaña de nitrógeno activa se entregó a través de anuncios maliciosos para PuTTY y FileZilla

Se ha observado una campaña en curso dirigida a administradores de sistemas con anuncios fraudulentos de utilidades de sistema populares. Los anuncios maliciosos se muestran como resultados patrocinados en la página del motor de búsqueda de Google y se localizan en América del Norte.

Prioridad: 1 Crítico.

Ampliar información:

https://www.malwarebytes.com/blog/threat-intelligence/2024/04/active-nitrogen-campaign-delivered-via-malicious-ads-for-putty-filezilla

---

Ransomware DragonForce

Una variante relativamente reciente de ransomware conocida como DragonForce ha estado en los titulares tras una serie de ataques de alto perfil. Al igual que muchos otros

grupos de ransomware, DragonForce busca extorsionar dinero de sus víctimas de dos maneras: mediante el bloqueo de acceso a computadoras y datos de empresas a través del cifrado, y la exfiltración de datos de sistemas comprometidos con la amenaza de su divulgación en la dark web.

Prioridad: 3 Importante.

Ampliar información:

https://www.tripwire.com/state-of-security/dragonforce-ransomware-what-you-need-know

---

El ataque de phishing TA547 ataca a empresas alemanas con el ladrón "Rhadamanthys"

El grupo de amenazas conocido como TA547 ha dirigido una serie de ataques contra numerosas organizaciones alemanas utilizando el ladrón de información Rhadamanthys como parte de una campaña de phishing centrada en facturas. Este incidente marca la primera vez que los investigadores identifican a TA547 empleando Rhadamanthys, un ladrón de información comúnmente utilizado por varios grupos cibercriminales.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/ta547-phishing-attack-hits-german-firms.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

Home Depot confirma que una brecha de datos de un tercero expuso información de empleados

Home Depot ha confirmado que sufrió una brecha de datos después de que uno de sus proveedores de software como servicio (SaaS) expusiera por error una pequeña muestra de datos limitados de empleados, los cuales podrían ser utilizados en ataques de phishing dirigidos.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/home-depot-confirms-third-party-data-breach-exposed-employee-info/

Los hackers pueden usar alucinaciones de IA para propagar malware

La inteligencia artificial generativa es experta en sonar autoritaria, incluso cuando está inventando información. Abogados incautos han presentado escritos judiciales haciendo referencia a precedentes legales inventados de la nada. El medio de noticias CNET emitió una corrección después de publicar consejos de finanzas personales extremadamente inexactos generados por IA.

Prioridad: 3 Importante.

Ampliar información:

https://www.bankinfosecurity.com/hackers-use-ai-hallucinations-to-spread-malware-a-24793

Ransomware CL0P: Medidas de seguridad para 2024

Surgiendo a principios de 2019, CL0P fue presentado inicialmente como una versión más avanzada de su predecesor, el ransomware 'CryptoMix', desarrollado por su propietario, CL0P Ransomware, una organización cibercriminal. A lo largo de los años, el grupo se mantuvo activo con campañas significativas desde 2020 hasta 2022. Sin embargo, en 2023, la banda de ransomware CL0P llevó sus actividades a nuevas alturas, convirtiéndose en una de las organizaciones de ransomware más activas y exitosas del mundo.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/04/cl0ps-ransomware-rampage-security.html