GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0824

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

VULNERABILIDADES

Cómo afecta CVE-2023 a la mayoría de los sistemas de LINUX

CVE-2023-40547 es una vulnerabilidad crítica en shim, un componente esencial del proceso de arranque seguro en la mayoría de las distribuciones de Linux. Descubierta por Bill Demirkapi y reportada al Centro de Respuesta de Seguridad de Microsoft, esta vulnerabilidad se origina en el manejo del protocolo HTTP, lo que puede resultar en una escritura fuera de los límites y comprometer completamente el sistema.

Prioridad: 1 Critico.

Ampliar información:

https://eclypsium.com/blog/the-real-shim-shady-how-cve-2023-40547-impacts-most-linux-systems/

Vulnerabilidad de escala de privilegios locales en VMvare

El producto VMware Aria Operations for Networks presenta una vulnerabilidad crítica de escalada de privilegios locales, identificada como CVE-2024-22237. Si un usuario de consola aprovecha esta vulnerabilidad, podría escalar sus privilegios y obtener acceso root en el sistema. Es fundamental abordar esta vulnerabilidad de inmediato para evitar posibles intrusiones no autorizadas. Prioridad: 2 Urgente.

Prioridad: 3 Importante.

Ampliar información:

https://www.vmware.com/security/advisories/VMSA-2024-0002.html

---

CVE-2024-22024 - XXE vulnerabilidad en productos Ivanti

CVE-2023-40547 es una vulnerabilidad crítica en shim, un componente esencial del proceso de arranque seguro en la mayoría de las distribuciones de Linux. Descubierta por Bill Demirkapi y reportada al Centro de Respuesta de Seguridad de Microsoft, esta vulnerabilidad se origina en el manejo del protocolo HTTP, lo que puede resultar en una escritura fuera de los límites y comprometer completamente el sistema.

Prioridad: 3 Importante.

Ampliar información:

https://www.akamai.com/blog/security-research/2024/feb/scanning-activity-ivanti-cve-february-2024

Akira y Lockbit están buscando dispositivos vulnerables de CISCO ASA

Los grupos de ransomware Akira y Lockbit están explotando vulnerabilidades antiguas en dispositivos Cisco ASA SSL VPN. El investigador Kevin Beaumont advierte sobre la necesidad de aplicar parches disponibles desde 2020 y 2023. Destaca la falta de visibilidad completa sobre los exploits existentes. Recomienda actualizar a la última versión de ASA en todos los dispositivos con la función de VPN SSL AnyConnect habilitada en la interfaz expuesta a internet.

Prioridad: 1 Crítico.

Ampliar información:

https://www.helpnetsecurity.com/2024/02/08/ransomware-cisco-asa-vulnerabilitiees/

Falla de VPN SSL FortiOS de Fortinet

Fortinet reveló una vulnerabilidad crítica en FortiOS SSL VPN, CVE-2024-21762, que posiblemente esté siendo explotada en ataques en curso. Esta vulnerabilidad, con una puntuación CVSS de 9.6, permite la ejecución de código y comandos arbitrarios a través de solicitudes HTTP manipuladas. La compañía advierte que el problema podría estar siendo explotado en la naturaleza, aunque no proporcionó detalles sobre los ataques en curso. Es crucial tomar medidas inmediatas para mitigar esta amenaza.

Prioridad: 1 Critico.

Ampliar información:

https://thehackernews.com/2024/02/fortinet-warns-of-critical-fortios-ssl.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

Blueshell utilizado en ataques contra sistemas linux en Corea

El Centro de Inteligencia de Seguridad de AhnLab (ASEC) ha detectado variantes de malware BlueShell utilizadas en ataques específicos contra sistemas Linux en Tailandia y Corea. Estos ataques implicaron la adaptación del malware de puerta trasera BlueShell por

parte de los actores de amenazas cibernéticas, quienes lo configuraron para funcionar únicamente en los sistemas específicos.

Prioridad: 3 Importante.

Ampliar información:

https://asec.ahnlab.com/en/61549/

El Malware Coyote y 61 aplicaciones bancarias

Los investigadores han revelado la presencia de un nuevo troyano bancario llamado "Coyote", diseñado para obtener credenciales de acceso a 61 aplicaciones bancarias. Este hallazgo es de un análisis reciente de Kaspersky donde destaca la amplitud de su enfoque en las aplicaciones bancarias, especialmente en Brasil, así como su compleja combinación de tecnologías, que incluye el nuevo instalador de código abierto Squirrel, NodeJs, el lenguaje de programación "Nim" y más de una docena de funciones maliciosas. Esta evolución en el mercado brasileño de malware financiero plantea desafíos significativos para los equipos de seguridad en el futuro si "Coyote" amplía su alcance.

Prioridad: 3 Importante.

Ampliar información:

https://www.darkreading.com/threat-intelligence/coyote-malware-preying-61-banking-apps

---

Malware RAT disfrazado

El Centro de Inteligencia de Seguridad de AhnLab (ASEC) ha identificado la distribución de un malware RAT disfrazado como un archivo ilegal relacionado con los juegos de azar. Siguiendo un método similar al utilizado por VenomRAT el mes pasado, este malware se

propaga a través de archivos de acceso directo (.lnk) y descarga el RAT directamente desde un archivo HTA. Es crucial estar alerta ante esta nueva amenaza y tomar medidas proactivas para proteger los sistemas contra posibles ataques.

Prioridad: 1 Crítico.

Ampliar información:

https://asec.ahnlab.com/en/61335

Malware como servicio principal amenaza para las organizaciones

Las infecciones de Malware como Servicio (MaaS) fueron la mayor amenaza para las organizaciones en la segunda mitad de 2023, según un informe de Darktrace. Destacó la adaptación multifuncional de muchas cepas de malware, combinando cargadores como troyanos de acceso remoto (RATs) con malware de robo de información. Darktrace encontró que estas cepas de malware se desarrollan con al menos dos funciones y son compatibles con varias herramientas existentes, lo que las hace especialmente peligrosas ya que pueden recolectar datos y credenciales sin exfiltrar archivos, dificultando su detección.

Prioridad: 2 Urgente.

Ampliar información:

https://www.infosecurity-magazine.com/news/malware-service-top-threat/

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

TinyTurla próxima Generación - Turla APT espía a ONG polacas

Talos, en cooperación con CERT.NGO, investigó otro compromiso del actor de Turla, con una nueva puerta trasero bastante similar a TinyTurla, que estamos llamando TinyTurla-NG (TTNG). Nuestras conclusiones indican que las organizaciones no gubernamentales polacas están siendo objeto de un objeto de atención, y al menos una de ellas apoya a Ucrania. Si bien las ONG no participan directamente en conflictos, con frecuencia participan

en la prestación de ayuda a las entidades que sufren a través de los conflictos. Las partes agresoras pueden considerar estratégicamente beneficioso supervisar a esas ONG para hacer un seguimiento de los paquetes de ayuda en curso y potencialmente nuevos para sus víctimas.

Prioridad: 3 Importante.

Ampliar información:

https://blog.talosintelligence.com/tinyturla-next-generation/

Ciberataques de Ucrania a Rusia en las operaciones terrestres

Después de la invasión rusa, Ucrania ha reevaluado su estrategia de ciberseguridad y ha adoptado un enfoque más proactivo. En lugar de simplemente defender sus sistemas, Ucrania ahora está llevando a cabo operaciones para hackear empresas estatales y privadas rusas, con el fin de recopilar información valiosa. Este cambio de enfoque no solo busca prevenir futuros ciberataques, sino también apoyar operaciones en territorios ocupados o en Rusia. Según Illia Vitiuk, jefe de ciberseguridad del Servicio de Seguridad de Ucrania, este enfoque, conocido como "defender hacia adelante", es fundamental en la estrategia cibernética de EE. UU., que busca neutralizar las capacidades cibernéticas del adversario para evitar ciberataques destructivos.

Prioridad: 3 Importante.

Ampliar información:

https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia/

DoJ desmantela infraestructura de zona de guerra RAT

El Departamento de Justicia (DoJ) anunció la confiscación de la infraestructura en línea empleada para comercializar el troyano de acceso remoto (RAT) conocido como Warzone RAT. Los dominios www.warzone[.]ws y otros tres fueron utilizados para la venta de malware, el cual permitía a los ciberdelincuentes acceder y robar datos de forma clandestina. En una operación coordinada a nivel internacional, las fuerzas del orden arrestaron y acusaron a dos individuos en Malta y Nigeria por su participación en la distribución y respaldo del malware, así como por ayudar a otros ciberdelincuentes a utilizar el RAT con fines maliciosos.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/us-doj-dismantles-warzone-rat.html

---

Coalición contra el ciber espionaje en el software comercial

Una coalición de países, entre los que se encuentran Francia, el Reino Unido y los Estados Unidos, junto con empresas tecnológicas como Google, MDSec, Meta y Microsoft, han firmado el acuerdo conjunto conocido como Proceso de Pall Mall. Este esfuerzo tiene como objetivo frenar el abuso de software espía comercial para violaciones de los derechos humanos. La iniciativa busca abordar la proliferación y el uso irresponsable de herramientas de intrusión cibernética comerciales, estableciendo principios rectores y opciones de políticas para Estados, la industria y la sociedad civil relacionados con su desarrollo, facilitación, compra y uso.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/02/global-coalition-and-tech-giants-unite.html

---