GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2623

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

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	1	
MALWARE	1	2	1
BRECHAS DE SEGURIDAD		1	1
NOTICIAS DE CIBERSEGURIDAD	1	1	1
SECTOR FINANCIERO		1	

VULNERABILIDADES

Stack Rot, nueva vulnerabilidad del kernel de Linux (CVE-2023-3269)

Se ha descubierto una vulnerabilidad crítica en el Kernel de Linux hasta la versión 6.4. Esta vulnerabilidad, conocida como Stack Rot, afecta al subsistema de administración de memoria y se encuentra en el componente de Expansión de Pila. A través de la manipulación de un input desconocido, se puede producir un desbordamiento de búfer. El problema principal se encuentra en el "maple tree", una nueva estructura de datos introducida en la versión 6.1 del Kernel de Linux. Esta vulnerabilidad afecta a casi todas las configuraciones del Kernel y se considera difícil de explotar. Se

espera que a fines de julio se publiquen una Prueba de Concepto (PoC) y más detalles técnicos sobre este error.

Prioridad: 1 Crítico.

Ampliar información:

- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1643/
- https://vuldb.com/es/?id.232986

Vulnerabilidad crítica para FortiNAC (CVE-2023-33299 y CVE-2023-33300)

Se han identificado dos vulnerabilidades en FortiNAC, conocidas como CVE-2023-33299 y CVE-2023-33300. La primera, con un puntaje CVSS de 9.6, es una vulnerabilidad de deserialización de datos no confiables.

Por otro lado, la vulnerabilidad CVE-2023-33300, con un puntaje CVSS de 4.8, se trata de una vulnerabilidad de inyección de comandos debido a la neutralización incorrecta de elementos especiales en los comandos utilizados. Las versiones afectadas se detallan a continuación y se recomienda a los usuarios que actualicen a las versiones no afectadas correspondientes:

- 9.4.0 - 9.4.3: actualizar a 9.4.4
- 9.2.0 - 9.2.7: actualizar a 9.2.8
- 9.1.0 - 9.1.9: actualizar a 9.1.10
- 7.2.0 - 7.2.2: actualizar a 7.2.3
- 8.3 - 8.8: actualizar a una versión no afectada.

Prioridad: 1 Crítico.

Ampliar información:

- https://es-la.tenable.com/blog/cve-2023-33299-critical-remote-code-execution-vulnerability-in-fortinac

- https://blog.segu-info.com.ar/2023/07/otra-vulnerabilidad-critica-para.html
- https://frycos.github.io/vulns4free/2023/06/18/fortinac.html

---

Vulnerabilidad de autenticación de omisión de SD-WAN de VMware (CVE-2023-20899)

Se ha descubierto una vulnerabilidad de omisión de autenticación en VMware SD-WAN (Perímetro). La vulnerabilidad, identificada como CVE-2023-20899, ha sido evaluada como moderada, con una puntuación base CVSSv3 máxima de 5.3. Un atacante no autenticado puede aprovechar esta vulnerabilidad para descargar el paquete de diagnóstico de la aplicación en VMware SD-WAN Management. Se recomienda a los usuarios afectados que apliquen las actualizaciones indicadas en la "Matriz de respuestas". Es importante tener en cuenta que esta vulnerabilidad solo afecta a los dispositivos Edge y no a la consola de administración SD-WAN (VCO). No se han identificado soluciones alternativas ni documentación adicional en relación con esta vulnerabilidad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.vmware.com/security/advisories/VMSA-2023-0015.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-20899

Vulnerabilidad en Apache Johnzon hasta 1.2.20 (CVE-2023-33008)

Se ha descubierto una vulnerabilidad de deserialización de datos no confiables en Apache Johnzon, una biblioteca de procesamiento JSON de Apache Software Foundation. Un atacante malintencionado puede crear una entrada JSON utilizando números grandes, como 1e20000000, que Apache Johnzon deserializará en objetos BigDecimal. Esto puede llevar a un consumo excesivo de recursos y una conversión lenta, lo que representa un riesgo de denegación de servicio. Para mitigar este problema, la versión 1.2.21 de Apache Johnzon ha establecido un límite de escala

predeterminado de 1000 para los objetos BigDecimal. Se ha confirmado que esta vulnerabilidad afecta a las versiones de Apache Johnzon anteriores a 1.2.20.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-33008

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

BlackByte 2.0 Ransomware: infiltra, cifra y extorsiona en solo 5 días

Los ataques de ransomware BlackByte 2.0 se están intensificando, con los piratas informáticos completando el proceso en solo cinco días. Utilizan vulnerabilidades en los servidores de Microsoft Exchange sin parches y técnicas de evasión para cifrar los datos y exigir rescate. Microsoft insta a las organizaciones a implementar parches de seguridad y protección contra manipulaciones para defenderse de estos ataques.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/
- https://thehackernews.com/2023/07/blackbyte-20-ransomware-infiltrate.html?&web_view=true

---

Variante del malware 'RustBucket' afecta a usuarios de macOS

Esta versión actualizada, creada por el grupo de hackers norcoreano BlueNoroff, aprovecha una infraestructura de red dinámica para el comando y control del malware. RustBucket fue identificado por primera vez en abril de 2023 y se trata de una puerta trasera basada en AppleScript que puede descargar una carga útil adicional desde un servidor remoto. El malware secundario, compilado en Swift, tiene la capacidad de descargar el binario principal basado en Rust desde el servidor de comando y control, recopilar información y ejecutar otros binarios o scripts de shell en el sistema comprometido.

Prioridad: 2 Urgente.

Ampliar información:

- https://malwaretips.com/threads/beware-new-rustbucket-malware-variant-targeting-macos-users.124196/

- https://thehackernews.com/2023/07/beware-new-rustbucket-malware-variant.html

---

Los actores de amenazas de Crysis usan conexiones RDP para distribuir el ransomware Venus

El ransomware Crysis ha utilizado conexiones de Protocolo de Escritorio Remoto (RDP) para distribuir el ransomware Venus. Este incidente destaca la necesidad de fortalecer la seguridad de las conexiones RDP para evitar compromisos y salvaguardar la información empresarial. Implementar medidas como autenticación multifactor y monitoreo constante de las conexiones RDP es crucial para prevenir estos ataques cibernéticos.

Prioridad: 3 Importante.

Ampliar información:

- https://cyware.com/news/crysis-threat-actors-use-rdp-connections-to-distribute-venus-ransomware-bddeda1ehttps://thehackernews.com/2023/07/beware-new-rustbucket-malware-variant.html

---

RedEnergy: Nuevo Stealer-as-a-Ransomware

Los investigadores de Zscaler ThreatLabz han descubierto RedEnergy, un nuevo malware que combina características de un stealer (ladrón de datos) y ransomware. Este malware se ha utilizado en ataques dirigidos a empresas de energía, petróleo y gas, telecomunicaciones y maquinaria. RedEnergy utiliza campañas de actualización falsas como táctica principal para infiltrarse en diversas industrias. Una vez comprometido un sistema, el malware extrae información confidencial y luego cifra los archivos. Los atacantes utilizan técnicas de ofuscación y se comunican a través de HTTPS para dificultar la detección. Además, eliminan datos de copias de seguridad y de shadow drive.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/redenergy-new-stealer-as-a-ransomware-out-in-the-wild-6ab8cc7c
- https://heimdalsecurity.com/blog/redenergy-stealer-ransomware-a-new-threat-targeting-critical-infrastructure/

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.

BRECHAS DE SEGURIDAD

Microsoft niega la afirmación de Anonymous Sudan sobre una supuesta violación de datos

Microsoft niega la afirmación de Anonymous Sudan de haber pirateado la empresa y obtenido acceso a más de 30 millones de cuentas de clientes. A principios de junio, Microsoft experimentó interrupciones en varios servicios debido a ataques DDoS, que Anonymous Sudan se atribuyó. Aunque el grupo afirmó haber robado las credenciales de 30 millones de cuentas, Microsoft ha declarado que no ha visto ninguna evidencia de acceso o compromiso de datos de los clientes. La empresa ha negado categóricamente la violación de datos y no ha comentado públicamente sobre el supuesto incidente.

Prioridad: 3 Importante.

Ampliar información:

- https://securityaffairs.com/148119/hacktivism/anonymous-sudan-claims-stolen-microsoft-data.html?web_view=true
- https://www.infosecurity-magazine.com/news/microsoft-denies-major-30-million/?&web_view=true

---

El puerto japonés de Nagoya suspende operaciones después de sufrir un ataque de ransomware

El puerto más grande de Japón en términos de capacidad de carga, Nagoya ha detenido la carga y descarga de mercancías debido a un incidente que afectó su sistema informático. Se cree que la banda de ransomware LockBit 3.0 está detrás del ataque, aunque no está claro si se robaron datos del puerto. Las autoridades portuarias están trabajando para restaurar los sistemas y se espera que las operaciones se reanuden pronto. Este incidente destaca la creciente preocupación por los ciberataques y la necesidad de mejorar la seguridad informática

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/japans-nagoya-port-suspends-cargo-operations-following-ransomware-attack/
- https://www.eleconomista.net/actualidad/El-puerto-mas-grande-de-Japon-detiene-sus-operaciones-por-un-ciberataque-20230706-0006.html

NOTICIAS DE CIBERSEGURIDAD

MITRE revela las 25 debilidades de software más peligrosas de 2023

MITRE ha publicado su lista anual de las 25 debilidades de software más peligrosas para el año 2023. Estas debilidades pueden llevar a vulnerabilidades graves en el software, permitiendo a los atacantes tomar el control de sistemas, robar datos o interrumpir el funcionamiento de las aplicaciones. La lista se basa en un análisis de datos públicos de vulnerabilidades y se asignó una puntuación a cada una en función de su prevalencia y gravedad. Algunas de las principales debilidades incluyen la escritura fuera de los límites, secuencias de comandos entre sitios, inyección de SQL y uso después de la liberación.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/06/mitre-unveils-top-25-most-dangerous.html
- https://cwe.mitre.org/top25/
- https://cwe.mitre.org/news/archives/news2023.html#june29_2023_CWE_Top_25_Now_Available

Mozilla ha lanzado Firefox 115 con parches para una docena de vulnerabilidades

Mozilla lanza Firefox 115 con parches para una docena de vulnerabilidades, incluyendo errores de uso después de la liberación de alta gravedad. Estas vulnerabilidades afectan a la generación de certificados WebRTC y al motor de código abierto JavaScript y WebAssembly SpiderMonkey. Los parches también abordan errores de seguridad de memoria que podrían permitir la ejecución de código arbitrario. Además, se han solucionado ocho vulnerabilidades de gravedad media que podrían conducir a ataques de suplantación de identidad, descarga de archivos maliciosos y engaño a los usuarios para enviar datos confidenciales.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/firefox-115-patches-high-severity-use-after-free-vulnerabilities/?web_view=true
- https://www.mozilla.org/en-US/security/advisories/

La Unión Europea ya ha elegido a los 7 Gatekeepers

La Unión Europea ha seleccionado a los siete 'Gatekeepers' o Guardianes de Acceso como parte de la Ley de Mercados Digitales. Estas empresas son Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta, Microsoft y Samsung. El objetivo de esta ley es combatir el abuso de poder de las grandes compañías tecnológicas y garantizar la libertad de elección de los usuarios. Los 'Gatekeepers' ya no podrán imponer su ecosistema a los usuarios, decidir qué aplicaciones deben tener preinstaladas o qué tiendas de aplicaciones deben utilizar. Además, se les exigirá que sus aplicaciones de mensajería sean interoperables con otras. Esta legislación representa un cambio significativo en la forma en que los ciudadanos europeos utilizarán Internet y las aplicaciones en el futuro.

Prioridad: 3 Importante.

Ampliar información:

- https://blog.elhacker.net/2023/07/la-union-europea-ya-ha-elegido-los-7-gatekeepers.html
- https://computerhoy.com/internet/union-europea-gatekeepers-ley-mercados-digitales-1271062