GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3023

En alianza con

TD SYNNEX FORTINET

BOLETIN 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	1	
MALWARE	1	2	1
BRECHAS DE SEGURIDAD			
NOTICIAS DE CIBERSEGURIDAD	1	2	3

VULNERABILIDADES

Múltiples vulnerabilidades en PHP

El 4 de agosto de 2023 se informó sobre múltiples vulnerabilidades en PHP, específicamente en las versiones 8.1.x anteriores a 8.1.22. Estas vulnerabilidades podrían permitir a un atacante provocar problemas de seguridad no especificados por el editor y evadir políticas de seguridad. Se recomienda consultar el boletín de seguridad del editor para obtener los parches necesarios.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0621/

Vulnerabilidad de OpenSSH CVE-2023-38408

El 2 de agosto de 2023, se reveló una vulnerabilidad en OpenSSH, identificada como CVE-2023-38408. Afecta la función PKCS#11 en ssh-agent en versiones previas a la 9.3p2 de OpenSSH, permitiendo ejecución remota de código si un agente SSH es reenviado a un sistema controlado por un atacante. Esta amenaza surge de una ruta de búsqueda poco confiable en la que el código en /usr/lib puede no ser seguro para cargar en ssh-agent. Esta vulnerabilidad persiste debido a una corrección incompleta para CVE-2016-10009. Su explotación podría permitir a atacantes ejecutar código en sistemas objetivo.

Prioridad: 1 Crítico.

Ampliar información:

- https://my.f5.com/manage/s/article/K000135709?utm_source=f5support&utm_medium=RSS

Vulnerabilidades de OpenJDK CVE-2023-22006, CVE-2023-22043 y CVE-2023-22045

El 2 de agosto de 2023, se reportaron tres vulnerabilidades en Oracle Java SE, Oracle GraalVM Enterprise Edition y Oracle GraalVM para JDK, identificadas como CVE-2023-22006, CVE-2023-22043 y CVE-2023-22045. Los ataques exitosos requieren interacción humana por parte de alguien que no sea el atacante. Las consecuencias de una explotación exitosa incluyen el acceso no autorizado para actualizar, insertar o eliminar datos accesibles de los productos afectados. Sin embargo, los productos de F5 no se ven afectados por estas vulnerabilidades y no hay impacto en ellos.

Prioridad: 1 Crítico.

Ampliar información:

- https://my.f5.com/manage/s/article/K000135718?utm_source=f5support&utm_medium=RSS%7D

Múltiples vulnerabilidades en productos de Mozilla

El 3 de agosto de 2023 se reportaron múltiples vulnerabilidades en productos de Mozilla. Estas vulnerabilidades podrían ser aprovechadas por un atacante remoto para desencadenar una condición de denegación de servicio, elevación de privilegios, ejecución remota de código, bypass de restricciones de seguridad y divulgación de información sensible en el sistema objetivo.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/mozilla-products-multiple-vulnerabilities_20230803
- https://www.mozilla.org/en-US/security/advisories/

Múltiples Vulnerabilidades en RedHat Linux Kernel

En RedHat Linux Kernel se han identificado múltiples vulnerabilidades que podrían permitir a un atacante remoto realizar denegación de servicio, elevar privilegios y evadir restricciones de seguridad en sistemas afectados. Esto afecta a diversas versiones y arquitecturas de Red Hat, incluyendo Red Hat CodeReady Linux Builder y Red Hat Enterprise Linux. Se recomienda aplicar las soluciones proporcionadas por el proveedor para abordar estas vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/redhat-linux-kernel-multiple-vulnerabilities_20230802

Error crítico de PaperCut expone servidores sin parches a ataques RCE

Un reciente informe revela que PaperCut, un software de gestión de impresión ha solucionado una vulnerabilidad crítica en su software NG/MF que permite a atacantes sin autenticación ejecutar código remoto en servidores Windows no parcheados. Identificada como CVE-2023-39143, la falla se origina en dos debilidades de recorrido de ruta que posibilitan a los atacantes leer, eliminar y subir archivos arbitrarios sin interacción del usuario. Aunque solo afecta a servidores con configuraciones no predeterminadas, muchos servidores PaperCut tienen esta configuración habilitada por defecto.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/new-papercut-critical-bug-exposes-unpatched-servers-to-rce-attacks/

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

Nueva variante de malware SkidMap dirigida a servidores Redis vulnerables

Un nuevo y peligroso malware llamado SkidMap ha sido descubierto atacando servicios vulnerables de Redis en diversas distribuciones de Linux. Esta variante del malware, que se adapta al sistema en el que se ejecuta, tiene como objetivo distribuciones como Alibaba, Anolis, openEuler, EulerOS, Stream, CentOS, RedHat y Rocky. SkidMap, originalmente identificado en 2019 como un botnet de minería de criptomonedas, ahora despliega un script para distribuir un archivo binario ELF disfrazado de imagen GIF, el cual añade claves SSH, deshabilita SELinux y establece un shell inverso que se comunica con un servidor controlado por los atacantes. Además, el malware descarga un paquete específico según la distribución de Linux y el kernel utilizado, y presenta avanzadas capacidades para ocultar sus actividades y camuflarse en los sistemas infectados.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/08/new-skidmap-redis-malware-variant.html?&web_view=true

---

Aplicaciones maliciosas utilizan una técnica de control de versiones furtiva para eludir los escáneres de Google Play Store

Los hackers están usando "versioning" para eludir la detección de malware en Google Play Store y atacar a usuarios de Android. Esta táctica implica lanzar una versión inicial de una app que pasa los controles de Google, pero luego se actualiza con malware. El malware disfrazado de apps aparentemente inofensivas también se ha detectado. Se recomienda a los usuarios de Android descargar solo de fuentes confiables y habilitar Google Play Protect para recibir alertas sobre apps dañinas.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/08/malicious-apps-use-sneaky-versioning.html?&web_view=true

---

Chrome malware Rilide se dirige a usuarios empresariales a través de guías de PowerPoint

La extensión maliciosa Rilide Stealer para Chrome ha regresado en nuevas campañas dirigidas a usuarios empresariales y de criptomonedas para robar credenciales y carteras de criptomonedas. Esta extensión maliciosa, descubierta inicialmente en abril de 2023, se disfraza de extensiones legítimas de Google Drive para secuestrar el navegador y robar información como credenciales de correo electrónico o activos de criptomonedas. La última versión de Rilide ahora también apunta a cuentas bancarias y puede exfiltrar datos robados a través de un canal de Telegram o tomando capturas de pantalla y enviándolas al servidor C2. A pesar de los intentos de Google por limitar su actividad, Rilide se adapta a estas restricciones y se mantiene activa, afectando a múltiples sectores y utilizando diversas técnicas de distribución y engaño. La popularidad y disponibilidad de esta amenaza en foros de hackers la hacen difícil de rastrear y prevenir.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/chrome-malware-rilide-targets-enterprise-users-via-powerpoint-guides/

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

Burger King expuso credenciales sensibles

Burger King ha expuesto nuevamente datos sensibles al público debido a una configuración incorrecta en su sitio web, poniendo en riesgo sus sistemas y datos. El equipo de investigación de Cybernews descubrió que la cadena de comida rápida en Francia expuso credenciales sensibles en un archivo (.env) que estaba públicamente accesible en su sitio web. Aunque estas credenciales por sí solas no habrían sido suficientes para tomar el control total del sitio, podrían haber facilitado un posible ataque cibernético a los sistemas de la cadena.

Prioridad: 3 Importante.

Ampliar información:

- https://cybernews.com/security/burger-king-data-leak/

NOTICIAS DE CIBERSEGURIDAD

Extrañas formas en que los empleados pueden exponer datos de forma accidental

En el artículo recomendado, se abordan formas inusuales en las que los empleados pueden exponer datos sensibles de manera accidental, desde reflejos en gafas durante videoconferencias hasta la revelación de información a través de fotos en redes sociales. Se destaca cómo acciones aparentemente inocentes pueden llevar a la exposición de datos corporativos y personales, subrayando la importancia de la educación en seguridad y la implementación de medidas preventivas.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.csoonline.com/article/573817/8-strange-ways-employees-can-accidently-expose-data.html

---

Qué está pasando en el mundo del Crimeware: Emotet, DarkGate y LokiBot

En el ámbito del crimeware, se ha detectado la presencia de nuevas variantes de malware como Emotet, el cargador "DarkGate" y la campaña del infostealer LokiBot. Estos hallazgos, detallados en informes privados, muestran la evolución constante del panorama de amenazas. DarkGate destaca

por sus avanzadas funcionalidades, mientras que LokiBot ha sido distribuido mediante campañas de phishing que aprovechan vulnerabilidades en documentos Excel.

Prioridad: 2 Urgente.

Ampliar información:

- https://securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/

Importancia de proteger sus contraseñas de redes sociales de hacks y ataques

Proteger sus cuentas de redes sociales de hackeos y ataques es crucial debido a las posibles consecuencias como fraude, desinformación y robo de datos personales. La autenticación de múltiples factores (MFA, por sus siglas en inglés) ofrece una fuerte defensa al agregar pasos adicionales al proceso de inicio de sesión, como códigos de un solo uso vía mensaje de texto o aplicaciones de autenticación, preguntas de seguridad o datos biométricos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.mcafee.com/blogs/privacy-identity-protection/protect-your-social-media-passwords-from-hacks-and-attacks/

Lazarus piratea fabricante de misiles ruso

El grupo de piratas informáticos Lazarus, vinculado a Corea del Norte, logró infiltrarse en las redes de un importante desarrollador ruso de misiles durante cinco meses el año pasado, según investigadores y evidencia técnica revisada por Reuters. Se encontraron pruebas de que los hackers instalaron puertas traseras en los sistemas de NPO Mashinostroyeniya, una oficina de diseño de cohetes en las afueras de Moscú. Aunque no se determinó qué datos se extrajeron, este incidente destaca cómo Corea del Norte apunta incluso a sus aliados para obtener tecnologías críticas. La empresa atacada, NPO Mash, es conocida por desarrollar misiles hipersónicos y tecnologías satelitales.

Prioridad: 3 Importante.

Ampliar información:

- https://cybernews.com/news/lazarus-hack-russia-missile-maker/?utm_source=twitter&utm_medium=social&utm_campaign=cybernews&utm_content=tweet

---

Amenazas de inteligencia artificial en la gestión de identidades

El Informe del Paisaje de Amenazas de Seguridad de Identidad 2023 de CyberArk revela preocupaciones entre profesionales de seguridad, incluyendo temores por amenazas internas y compromisos de identidad impulsados por factores financieros, geopolíticos y de nube. Se destaca el riesgo de ataques de inteligencia artificial (IA) en la proliferación de la identidad digital. La IA, al evolucionar más rápido que las defensas humanas, puede llevar a ataques altamente personalizados y erosionar la confianza en las identidades digitales. Esto sugiere la necesidad de enfoques estratégicos y operativos para limitar la cantidad de datos recopilados y fortalecer la confianza en las identidades digitales.

Prioridad: 3 Importante.

Ampliar información:

- https://securityintelligence.com/articles/artificial-intelligence-threats-in-identity-management/

Ataques globales de ransomware en su punto más alto, muestra el último informe sobre el estado del ransomware de 2023

Los ataques de ransomware continúan en aumento en 2023 según el informe del Estado del Ransomware de Malwarebytes. El informe revela que en un año se registraron 1,900 ataques de ransomware en cuatro países: Estados Unidos, Alemania, Francia y el Reino Unido. Estados Unidos

representa el 43% de todos los ataques globales, mientras que los ataques de ransomware en Francia casi se duplicaron en los últimos cinco meses. El Reino Unido también sufrió cerca de 200 ataques de ransomware. El informe destaca el ascenso del grupo CL0P, que utiliza vulnerabilidades de día cero para amplificar sus ataques, lo que podría cambiar el panorama del ransomware hacia un enfoque más agresivo y centrado en vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.redpacketsecurity.com/global-ransomware-attacks-at-an-all-time-high-shows-latest-state-of-ransomware-report/

Web 3.0: el futuro de Internet, sus características y desafíos de ciberseguridad

Web 3.0 es la próxima fase de Internet, descentralizada y con tecnologías como IA y blockchain. Ofrece mayor control de datos y aplicaciones descentralizadas, pero también trae riesgos nuevos como vulnerabilidades en contratos inteligentes y problemas de privacidad. Para enfrentar estos desafíos, es crucial incorporar la seguridad desde el diseño y elegir la cadena de bloques adecuada, además de estar al tanto de las últimas tendencias y buscar asesoramiento profesional.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.tripwire.com/state-of-security/web-3-future-internet-and-its-cybersecurity-features-and-challenges