GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º3623

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	3	1
MALWARE		3	
BRECHAS DE SEGURIDAD	1		
NOTICIAS DE CIBERSEGURIDAD	2	1	3
SECTOR GOBIERNO	1		

VULNERABILIDADES

Múltiples Vulnerabilidades en productos Cisco

Cisco Products presenta múltiples vulnerabilidades de seguridad, con un riesgo medio. Estas vulnerabilidades pueden permitir a atacantes remotos causar denegación de servicio, ejecución de código remoto, elusión de restricciones de seguridad y manipulación de datos en sistemas específicos. Los productos afectados incluyen routers de la Serie 8000, ASR 9000, software ASA anterior a 9.16.2.11 entre otros. Se recomienda aplicar las correcciones proporcionadas por Cisco para abordar estas vulnerabilidades. Los identificadores CVE asociados son CVE-2023-20135, CVE-2023-20190, CVE-2023-20191, CVE-2023-20233, CVE-2023-20236 y CVE-2023-20269.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20230915

Vulnerabilidades Múltiples en el Kernel de SUSE Linux

SUSE Linux Kernel presenta múltiples vulnerabilidades de riesgo medio. Un atacante remoto podría aprovechar algunas de estas vulnerabilidades para eludir restricciones de seguridad, causar una denegación de servicio, revelar información sensible, ejecutar código de forma remota y elevar privilegios en el sistema objetivo. Los sistemas y tecnologías afectados incluyen varias versiones de SUSE Linux Enterprise, SUSE Linux Enterprise Live Patching, SUSE Linux Enterprise Micro, SUSE Linux Enterprise Real Time, SUSE Linux Enterprise Server y más.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/suse-linux-kernel-multiple-vulnerabilities_20230915

Vulnerabilidad Crítica de Ejecución Remota en Mozilla

Se ha detectado una vulnerabilidad de ejecución remota de código en los productos de Mozilla, con un riesgo extremadamente alto. Un atacante remoto podría aprovechar esta vulnerabilidad, identificada como CVE-2023-4863, para ejecutar código de forma remota en el sistema afectado. Se destaca que ya existe un exploit en circulación para esta vulnerabilidad. Se recomienda a los usuarios actualizar a las siguientes versiones para mitigar el riesgo: Firefox 117.0.1, Firefox ESR 115.2.1, Firefox ESR 102.15.1, Thunderbird 102.15.1 y Thunderbird 115.2.2.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.hkcert.org/security-bulletin/mozilla-firefox-remote-code-execution-vulnerability_20230913

Vulnerabilidades en ChromeOS

ChromeOS presenta múltiples vulnerabilidades de riesgo medio que podrían permitir a atacantes remotos provocar una denegación de servicio, ejecución remota de código y revelación de información sensible en sistemas no actualizados a la versión 108.0.5359.242 (Versión de Plataforma: 15183.105.0). Se recomienda visitar el sitio web del proveedor para obtener más detalles y aplicar las correcciones proporcionadas por ChromeOS para abordar las vulnerabilidades identificadas como CVE-2023-4357 y CVE-2023-4362.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/chromeos-multiple-vulnerabilities_20230913

Vulnerabilidades en Biblioteca ncurses Afectan a Linux y macOS

Se han descubierto fallos de corrupción de memoria en la biblioteca de programación Ncurses, que podrían ser explotados por atacantes para ejecutar código malicioso en sistemas Linux y macOS. Estas vulnerabilidades, identificadas como CVE-2023-29491, se abordaron en abril de 2023, y Microsoft colaboró con Apple para solucionar los problemas específicos de macOS relacionados con estas fallas. Los atacantes podrían utilizar variables de entorno manipuladas para escalar privilegios en programas afectados.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/09/microsoft-uncovers-flaws-in-ncurses.html?&web_view=true

---

Vulnerabilidad 'ThemeBleed' en Windows 11 Expuesta

Se ha publicado un código de explotación de prueba de concepto para una vulnerabilidad en Windows 11 conocida como 'ThemeBleed' (CVE-2023-38146). Esto permite a atacantes ejecutar código malicioso si se abre un archivo .THEME manipulado. Aunque Microsoft ha solucionado el problema, aún persiste una condición de carrera, y no se han abordado las advertencias 'mark-of-the-web' para archivos .THEMEPACK. Se insta a los usuarios de Windows a aplicar las actualizaciones de seguridad de septiembre de 2023 lo antes posible.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/windows-11-themebleed-rce-bug-gets-proof-of-concept-exploit/?&web_view=true

---

Vulnerabilidades RCE en Kubernetes Exponen Windows Endpoints

Vulnerabilidades críticas en Kubernetes exponen endpoints de Windows a la ejecución remota de código (RCE). Akamai advierte a los administradores sobre estas amenazas que permiten a los atacantes tomar el control de sistemas no parcheados mediante inyección de comandos a través de archivos YAML maliciosos. Se insta a la acción inmediata para mitigar el riesgo.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/vulnerabilities-threats/kubernetes-admins-warned-to-patch-clusters-against-new-rce-vulns?&web_view=true

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

Nuevo Ransomware conocido como “3AM”

Se ha identificado una nueva familia de ransomware llamada 3AM que surgió como respuesta a un bloqueo de LockBit en una red objetivo. Escrito en Rust, este ransomware se utiliza en ataques limitados y presenta la extensión .threeamtime en los archivos cifrados. Aunque sus orígenes son desconocidos, su uso como respaldo por un afiliado de LockBit podría atraer la atención de otros ciberatacantes en el futuro.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/new-3am-ransomware-used-as-a-backup-to-lockbit-infection-9aae88d1/?web_view=true

---

MetaStealer: Nuevo Malware que Ataca a Usuarios de macOS

MetaStealer es un nuevo malware de robo de información que se dirige a sistemas macOS. Este software malicioso utiliza tácticas de ingeniería social para engañar a los usuarios empresariales de macOS y robar datos sensibles. A menudo, se disfraza como archivos y aplicaciones atractivas para atraer a las víctimas. Aunque algunas versiones de MetaStealer son detectadas por el antivirus de Apple, XProtect, las organizaciones deben estar alerta y tomar medidas de seguridad adicionales para protegerse contra esta amenaza en constante evolución.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/newly-discovered-metastealer-malware-targets-macos-users-1b87592f/?web_view=true

---

Nueva Variante de MidgeDropper

Se ha descubierto una variante no vista previamente del dropper llamado MidgeDropper, que presenta una cadena de infección compleja la cual incluye ofuscación de código y carga lateral, convirtiéndolo en un caso interesante de estudio. Aunque no se pudo obtener la carga final, esta investigación explora cómo opera este dropper. El vector de infección inicial parece estar relacionado con correos electrónicos de phishing que contienen un archivo RAR adjunto. El dropper desencadena una serie de acciones, descargando archivos y ejecutando procesos que, en última instancia, podrían permitir la instalación de malware adicional con diversos propósitos. Fortinet ya

proporciona protección contra este malware a través de varios de sus servicios, y se insta a las organizaciones a tomar medidas de seguridad adicionales contra amenazas de phishing.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.fortinet.com/blog/threat-research/new-midgedropper-variant?&web_view=true

---

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

Ataque de Ransomware Paraliza Entidades Gubernamentales en Colombia

Varias entidades gubernamentales colombianas, incluyendo el Ministerio de Salud y Protección Social, el Poder Judicial y la Superintendencia de Industria y Comercio, se ven afectadas por un ataque de ransomware que limita sus operaciones. El ataque, relacionado con el proveedor de tecnología IFX Networks Colombia, ha llevado a la suspensión de audiencias judiciales y la interrupción de servicios clave, lo que destaca la necesidad de una mayor atención a la ciberseguridad en el país.

Prioridad: 1 Crítico.

Ampliar información:

- https://therecord.media/colombia-government-ministries-cyberattack
- https://twitter.com/colCERT/status/1702908571925520633?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Etweet

---

NOTICIAS DE CIBERSEGURIDAD

Gamma Ingenieros posicionado entre los mejores 250 MSSP's en Ranking de MSSP Alert a nivel mundial

El ranking anual de MSSP Alert determina los principales proveedores de servicios en seguridad MSSP alrededor del mundo. En su versión 2023, Gamma Ingenieros ha sido reconocida como una de las dos únicas empresas colombianas que califican en este importante listado para el sector tecnológico.

Prioridad: 3 Importante.

Ampliar información:

- https://www.msspalert.com/top-250?utm_source=marketing-campaign&utm_medium=social&utm_campaign=250-list&utm_content=download-report

---

Modelo de Confianza Cero para Seguridad en la Nube según NIST

NIST publica SP 800-207A, un modelo de Confianza Cero para el control de acceso en aplicaciones en la nube. El documento destaca la importancia de establecer confianza en microservicios distribuidos y usuarios de diferentes ubicaciones a través de políticas de acceso y comunicación seguras. Recomienda una arquitectura de Confianza Cero (ZTA) con políticas dinámicas de autenticación y autorización, configuración de componentes tecnológicos y un marco de monitoreo para mejorar la seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.helpnetsecurity.com/2023/09/14/nist-sp-800-207a-zero-trust-architecture/?web_view=true

---

Microsoft Advierte sobre Nueva Campaña de Phishing en Teams

Microsoft ha alertado sobre una campaña de phishing que utiliza mensajes de Microsoft Teams para infiltrarse en redes corporativas. El grupo conocido como Storm-0324, o TA543, ha cambiado su enfoque y ahora distribuye cargas maliciosas a través de chats de Teams en lugar de correos electrónicos. La campaña busca aprovechar vulnerabilidades en la seguridad de Microsoft Teams para comprometer la red de las empresas y ha sido asociada con actividades de ransomware.

Prioridad: 1 Critico.

Ampliar información:

- https://thehackernews.com/2023/09/microsoft-warns-of-new-phishing.html?&web_view=true

---

Campaña de Phishing Sofisticada: Análisis de Ataque de Malware Remcos en Empresas Colombianas

Investigadores de Check Point han descubierto una sofisticada campaña de phishing que apunta a más de 40 empresas líderes en Colombia. Los atacantes utilizan correos electrónicos falsos que contienen archivos adjuntos maliciosos para instalar sigilosamente el malware Remcos en las computadoras de las víctimas. Este malware, una herramienta de administración remota, otorga a los atacantes un control completo sobre las máquinas infectadas, lo que plantea riesgos significativos de robo de datos y toma de control. El análisis detallado de esta investigación revela las tácticas y técnicas avanzadas utilizadas por los atacantes para evadir la detección, además, destaca la importancia de fortalecer las defensas cibernéticas contra tales amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://research.checkpoint.com/2023/guarding-against-the-unseen-investigating-a-stealthy-remcos-malware-attack-on-colombian-firms/?web_view=true

---

Exploit Pone en Riesgo Miles de Repositorios y Millones de Usuarios de GitHub

Se ha descubierto una nueva vulnerabilidad que podría permitir a un atacante explotar una condición de carrera en las operaciones de creación de repositorios y cambio de nombre de usuario en GitHub. Esta técnica podría utilizarse para llevar a cabo un ataque de Repojacking (secuestro de repositorios populares para distribuir código malicioso). Esta vulnerabilidad representa la cuarta vez que se identifica un método único que podría eludir el mecanismo de "retiro del espacio de nombres del repositorio popular" de GitHub. La vulnerabilidad se ha informado a GitHub y se ha solucionado. La explotación exitosa de esta vulnerabilidad podría permitir el secuestro de más de 4,000 paquetes

de código en lenguajes como Go, PHP y Swift, así como acciones de GitHub, lo que afectaría a millones de usuarios y numerosas aplicaciones.

Prioridad: 3 Importante.

Ampliar información:

- https://checkmarx.com/blog/persistent-threat-new-exploit-puts-thousands-of-github-repositories-and-millions-of-users-at-risk/?web_view=true

---

Nuevo generador cuántico de números aleatorios podría revolucionar la encriptación

Científicos de la Universidad de Linköping han desarrollado un nuevo tipo de generador cuántico de números aleatorios (QRNG) para la encriptación, que podría transformar la seguridad de las comunicaciones digitales. Este generador cuántico de números aleatorios utiliza diodos emisores de luz de perovskita y ofrece un alto nivel de seguridad y privacidad en la generación de claves de encriptación. La ventaja de esta tecnología es que podría ser más económica y respetuosa con el medio ambiente que las alternativas actuales basadas en láser. Se espera que este nuevo QRNG esté disponible para su uso en ciberseguridad dentro de cinco años, además podría desempeñar un papel fundamental en la protección de datos y la comunicación segura en el futuro.

Prioridad: 3 Importante.

Ampliar información:

- https://www.helpnetsecurity.com/2023/09/08/random-number-generator-encryption/?web_view=true