GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0624

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

VULNERABILIDADES

Alerta de seguridad en Mastodon: vullnerabilidad crítica descubierta

Mastodon emitió una llamada urgente a los administradores después de revelarse una vulnerabilidad crítica con una puntuación de gravedad de 9.4 (CVE-2024-23832). Esta amenaza podría permitir a los atacantes asumir el control remoto de cuentas en esta red social descentralizada. Las versiones afectadas abarcan desde la 3.5.17 hasta la 4.2.5, instando a los usuarios a actualizar de inmediato antes de la divulgación completa de detalles el 15 de febrero.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.theregister.com/2024/02/02/critical_vulnerability_in_mastodon_is/?&web_view=true

Vulnerabilidad Zero-Day en el registro de eventos de Windows

Una vulnerabilidad recientemente descubierta en el Registro de Eventos de Windows podría dejar expuestas las defensas empresariales. Aún sin parche, esta vulnerabilidad, puede bloquear el servicio de Registro de Eventos en varias versiones de Windows. Aunque no permite la ejecución remota de código, la falla proporciona sigilo temporal al detener el servicio, cegando las defensas basadas en registros de eventos de Windows. Mientras se espera el parche de Microsoft, los usuarios pueden utilizar microparches proporcionados por Acros para protegerse.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.helpnetsecurity.com/2024/01/31/windows-event-log-vulnerability/?web_view=true

---

Descubren nuevas vulnerabilidades en productos de Ivanti

La empresa de TI Ivanti, informó el descubrimiento de dos nuevas vulnerabilidades en sus productos durante la investigación de errores encontrados anteriormente. Las fallas afectan a los productos Ivanti Policy Secure y Ivanti Connect Secure VPN, ampliamente utilizados en el gobierno de EE. UU. y otras industrias. Las vulnerabilidades, denominadas CVE-2024-21888 y CVE-2024-21893, afectan a todas las versiones admitidas. La primera permite a un atacante elevar privilegios a administrador, mientras que la segunda posibilita el acceso a recursos restringidos sin autenticación. Aunque Ivanti lanzó parches, la advertencia de CISA destaca la persistencia de amenazas y la importancia de actualizaciones inmediatas en entornos gubernamentales y empresariales.

Prioridad: 1 Crítico.

Ampliar información:

- https://therecord.media/ivanti-warns-of-two-bugs-as-cisa-issues-alert-about-hackers?&web_view=true

CISA advierte sobre la explotación activa de una vulnerabilidad en Apple iOS y macOS

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) añadió una vulnerabilidad de alta gravedad que afecta a iOS, iPadOS, macOS, tvOS y watchOS a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV). La vulnerabilidad, identificada como CVE-2022-48618, reside en el componente del kernel y permite a un atacante con capacidad de lectura y escritura arbitraria eludir la Autenticación de Puntero. Apple señala que la vulnerabilidad podría haber sido explotada en versiones anteriores a iOS 15.7.1 y ha lanzado parches para abordar el problema. CISA insta a las agencias federales a aplicar las correcciones antes del 21 de febrero de 2024 debido a la evidencia de explotación activa.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/02/cisa-warns-of-active-exploitation-of.html?&web_view=true

Nueva vulnerabilidad en Glibc otorga acceso root en importantes distribuciones de Linux

Una reciente vulnerabilidad revelada en la biblioteca GNU C (glibc) plantea una seria amenaza, permitiendo a atacantes locales maliciosos obtener acceso completo como root en máquinas Linux. Identificada como CVE-2023-6246, la vulnerabilidad de desbordamiento de búfer basada en montón afecta a importantes distribuciones como Debian, Ubuntu y Fedora, impactando a sistemas que utilizan las funciones syslog() y vsyslog() para el registro. Aunque la explotación requiere condiciones específicas, el uso generalizado de la biblioteca afectada aumenta el riesgo. Los investigadores de Qualys también descubrieron dos fallas adicionales en la función

__vsyslog_internal() y un error de corrupción de memoria en la función qsort(), afectando a versiones de glibc desde 1992.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2024/01/new-glibc-flaw-grants-attackers-root.html?&web_view=true

---

Vulnerabilidad crítica en GitLab - Sobrescripción de archivos al crear espacios de trabajo

GitLab ha lanzado correcciones para abordar una grave vulnerabilidad en su Community Edition (CE) y Enterprise Edition (EE) que permitía a usuarios autenticados escribir archivos arbitrarios durante la creación de un espacio de trabajo. Identificada como CVE-2024-0402, la vulnerabilidad tiene una puntuación CVSS de 9.9. Se insta a los usuarios a actualizar a las versiones parcheadas (16.5.8, 16.6.6, 16.7.4, 16.8.1) para mitigar riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2024/01/urgent-upgrade-gitlab-critical.html?&web_view=true

---

Vulnerabilidades descubiertas por IOActive en cajeros automáticos de Bitcoin

Investigadores de seguridad de IOActive descubrieron vulnerabilidades (CVE-2024-0175, CVE-2024-0176, CVE-2024-0177) en cajeros automáticos de Bitcoin Lamassu Douro, permitiendo un control total. Tras obtener acceso al sistema durante el arranque, lograron una escalada de privilegios explotando el mecanismo de actualización de software, utilizando un código QR personalizado. Esto

les dió acceso de root, revelando contraseñas comunes para todos los dispositivos. El proveedor, Lamassu, solucionó los problemas después de la divulgación de IOActive.

Prioridad: 3 Importante.

Ampliar información:

- https://labs.ioactive.com/2024/01/atm-security-owning-bitcoin-atm.html?&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

Campaña de malware en macOS revela ingenioso método de distribución

Investigadores de seguridad han alertado sobre una nueva campaña de ciberataques que utiliza copias pirateadas de aplicaciones populares para distribuir un backdoor a usuarios de macOS. Lo distintivo de esta campaña radica en su escala y en una novedosa técnica de entrega de carga útil en varias etapas. El actor de amenazas utiliza hasta 70 aplicaciones macOS crackeadas, con títulos atractivos para usuarios empresariales, lo que pone en riesgo a organizaciones que no restringen las descargas de los usuarios. Aunque se especula sobre la posible formación de un botnet macOS, la campaña destaca por la amplia variedad de aplicaciones empresariales utilizadas como señuelo.

Prioridad: 3 Importante.

Ampliar información:

- https://www.darkreading.com/cyberattacks-data-breaches/macos-malware-campaign-showcases-novel-delivery-technique?&web_view=true

---

DarkGate Malware aprovecha Microsoft Teams en ataque de phishing

AT&T descubrió un ataque de phishing que utiliza el chat grupal de Microsoft Teams para distribuir el malware DarkGate. Los atacantes enviaron más de 1.000 invitaciones maliciosas, persuadiendo a los usuarios para que descarguen un archivo con una doble extensión engañosa. El malware, capaz de eludir Windows Defender, recibe comandos de su servidor de control en hgfdytrywq[.]com. Se recomienda a los usuarios estar alerta ante mensajes no solicitados en los que se pidan descargas y considerar desactivar el Acceso Externo en Microsoft Teams.

Prioridad: 2 Urgente.

Ampliar información:

- https://cyware.com/news/darkgate-malware-delivered-via-microsoft-teams-f7b25750/?web_view=true

---

Ransomware Python: amenaza en aumento

El uso de Python en ransomware está en alza, como revela una investigación reciente. Aunque el ransomware se compiló en Visual C++, el análisis estático reveló un componente crucial codificado en Python llamado "grinchv3.pyc". El comportamiento del ransomware, organizado bajo una clase "sweet", involucra la recopilación de información de la víctima, la persistencia en la carpeta de inicio y el cifrado de archivos en discos configurados utilizando el algoritmo Fernet. El análisis experimental confirmó la persistencia y mostró archivos cifrados con una extensión ".enc". La nota de rescate incluye instrucciones para desbloquear archivos, subrayando la importancia de la vigilancia del usuario, así como el uso de soluciones de seguridad confiables como "K7 Total Security".

Prioridad: 2 Urgente.

Ampliar información:

- https://labs.k7computing.com/index.php/pythons-byte-the-rise-of-scripted-ransomware/?web_view=true

---

Phobos Ransomware se expande con nueva variante FAUST

Investigadores de seguridad han descubierto una nueva variante del ransomware Phobos llamada FAUST. Esta variante utiliza un documento de Office para iniciar su ataque, con una cadena de infección que involucra comandos PowerShell, descargas ejecutables y cifrado de archivos. FAUST agrega la extensión .faust a los archivos cifrados, creando canales de negociación con las víctimas. Notablemente, excluye estratégicamente ciertos archivos y directorios del cifrado. A medida que el panorama de ransomware evoluciona, se insta a las organizaciones a mejorar la seguridad en los puntos finales, realizar copias de seguridad de datos regularmente y mantenerse alerta ante nuevas amenazas como FAUST.

Prioridad: 1 Crítico.

Ampliar información:

- https://cyware.com/news/phobos-ransomware-expands-with-new-faust-variant-096b0529/?web_view=true

---

Nuevo malware Android en Google Play: 12 aplicaciones descubiertas ejecutando VajraSpy RAT

Investigadores identificaron doce aplicaciones maliciosas en Android que ejecutan el troyano VajraSpy RAT, seis de las cuales estaban en Google Play. Estas aplicaciones comparten similitudes, incluyendo funciones de mensajería y certificados de desarrollador. Subidas entre abril de 2021 y marzo de 2023, las apps podrían haber afectado a alrededor de 1.400 usuarios. VajraSpy es un troyano personalizable capaz de exfiltrar datos. Las aplicaciones se dividen en tres grupos según sus funcionalidades. Algunas interceptan comunicaciones de WhatsApp y Signal. Se recomienda precaución al descargar aplicaciones, incluso de fuentes aparentemente confiables.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/android-malware-news-apps/#google_vignette

---

Recomendaciones generales sobre malware:

- Mantener los sistemas y aplicaciones 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

Ataques de phishing con señuelos de mensajes de voz

Los ciberdelincuentes están empleando una táctica novedosa para atraer a los usuarios hacia enlaces maliciosos: mensajes de voz falsos. En estos ataques, los hackers utilizan enlaces que parecen ser grabaciones de voicemails, dirigidos a usuarios corporativos con sistemas telefónicos vinculados a correos electrónicos. Al hacer clic en la supuesta grabación, los usuarios son redirigidos a páginas web maliciosas diseñadas para la recolección de credenciales.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.avanan.com/blog/fake-voicemail-as-credential-harvesting-lure?&web_view=true

---

AnyDesk confirma brecha de seguridad en sus servidores de producción

AnyDesk, una solución de acceso remoto, ha confirmado un reciente ciberataque que permitió a los hackers acceder a sus sistemas de producción. Durante el ataque, se robaron claves de firma de código y código fuente. Aunque AnyDesk no reveló si se sustrajo información, la firma de ciberseguridad CrowdStrike colaboró en la respuesta a la incidencia. A pesar de confirmar que no hubo ransomware, la compañía revocó certificados de seguridad, reemplazó sistemas y aseguró que AnyDesk sigue siendo seguro. Aunque no se robaron tokens de autenticación, AnyDesk recomienda cambiar las contraseñas como medida de precaución.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/?&web_view=true

---

Cloudflare hackeado por actor patrocinado posiblemente por un estado

Cloudflare reveló que un actor con credenciales robadas accedió a sus sistemas internos tras el hackeo de Okta en octubre de 2023. Aunque el acceso fue detectado el 23 de noviembre, las credenciales no se rotaron, permitiendo que los atacantes realizaran reconocimientos en los sistemas de Cloudflare. Aunque accedieron a AWS y Atlassian, la segmentación de red impidió el acceso a Okta y el panel de Cloudflare. No se encontró evidencia de acceso a la red global, base de datos de clientes o claves SSL. Cloudflare tomó medidas inmediatas, rotando más de 5.000 credenciales y mejorando la seguridad.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/cloudflare-hacked-by-suspected-state-sponsored-attacker/

Filtración de token en GitHub expone código fuente de Mercedes-Benz

Un token filtrado en el repositorio de GitHub de un empleado de Mercedes-Benz proporcionó acceso sin restricciones al código fuente en el servidor GitHub Enterprise de la empresa, según informes de RedHunt Labs. Descubierto en septiembre de 2023 y revocado en enero de 2024, el incidente podría haber permitido a los atacantes acceder a claves API, documentos de diseño y otra información crítica. La filtración plantea riesgos financieros, legales y de reputación.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/leaked-github-token-exposed-mercedes-source-code/
