GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4423

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín de ciberseguridad semanal 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, tecnología y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	4	1	
MALWARE	1	3	2
NOTICIAS DE CIBERSEGURIDAD		1	3

VULNERABILIDADES

Explotación Activa de Vulnerabilidad de Alta Gravedad en SLP

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incluido una vulnerabilidad de denegación de servicio (DoS) de alta gravedad en el Protocolo de Ubicación de Servicios (SLP) en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV). Identificada como CVE-2023-29552, la vulnerabilidad podría permitir a un atacante remoto no autenticado realizar ataques DoS con un factor de amplificación significativo.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html

Vulnerabilidades Críticas de Desbordamiento de Búfer en Módulos de Plataforma de Confianza de Trusted Computing Group (TCG)

Dos vulnerabilidades de desbordamiento de búfer han sido descubiertas en la especificación de la biblioteca de referencia del Módulo de Plataforma de Confianza (TPM) 2.0 del Trusted Computing Group. Estas vulnerabilidades permiten a los actores de amenazas acceder a datos sensibles de solo lectura o sobrescribir datos normalmente protegidos en el TPM. Los atacantes pueden aprovechar estas fallas enviando comandos específicamente diseñados al módulo. El Grupo de Computación Confiable ha lanzado una advertencia de seguridad, además, ha proporcionado parches para mitigar estos riesgos, afectando a varios proveedores y productos como libtpms, IBM, NetBSD, NixOS, Red Hat, Squid, SUSE Linux y Trusted Computing Group.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/trusted-platform-buffer-overflow/#google_vignette/

Vulnerabilidad de Inyección de Comandos en QNAP OS Permite la Ejecución de Comandos Maliciosos

Dos vulnerabilidades críticas de inyección de comandos en el sistema operativo QTS y aplicaciones asociadas de dispositivos de almacenamiento conectados a la red (NAS) de QNAP han sido descubiertas. Estas fallas podrían exponer información sensible, permitiendo a actores maliciosos ejecutar comandos remotos, lo que podría resultar en la filtración de datos y ser aprovechado para fines maliciosos, como demandas de rescate. QNAP ha lanzado avisos de seguridad y parches para abordar estas vulnerabilidades, asignadas como CVE-2023-23368 y CVE-2023-23369, ambas con severidades críticas. Se insta a los usuarios afectados a actualizar a las versiones más recientes para prevenir posibles explotaciones.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/qnap-os-command-injection-flaw/

Vulnerabilidades Críticas en Veeam Permiten la Ejecución Remota de Código y Robo de Hashes NTLM

Veeam, líder global en protección de datos, ha emitido parches para abordar cuatro vulnerabilidades en su plataforma de monitoreo y análisis de infraestructura de TI, Veeam ONE. Dos de estas vulnerabilidades se clasifican como críticas, permitiendo la ejecución remota de código y el robo de hashes NTLM. Las fallas críticas podrían conducir a la ejecución remota de código en el servidor SQL que aloja la base de datos de configuración de Veeam ONE, junto con la obtención del hash NTLM de la cuenta utilizada por el servicio de informes de Veeam ONE. Se recomienda a los usuarios afectados que apliquen los parches correspondientes para prevenir posibles explotaciones.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/veeam-critical-bug/

Vulnerabilidad Zero-Day en SysAid Explotada por Grupo de Ransomware

Se ha emitido una advertencia a las organizaciones que utilizan el software de gestión de servicios de TI SysAid sobre una vulnerabilidad zero-day que ha sido explotada por afiliados de una operación de ransomware notoria. La vulnerabilidad, identificada como CVE-2023-47246, es una cuestión de recorrido de ruta que lleva a la ejecución arbitraria de código. El equipo de inteligencia de amenazas de Microsoft fue el primero en observar la explotación del zero-day y notificó a SysAid, que lanzó una versión parcheada del software. Se ha atribuido la explotación de CVE-2023-47246 a un actor de amenazas conocido como Lace Tempest, vinculado previamente a ataques significativos de ransomware.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/sysaid-zero-day-vulnerability-exploited-by-ransomware-group/

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 Ataque de Malvertising Utiliza un Portal Falso de Noticias de Windows para Distribuir Malware

Un nuevo ataque de malvertising utiliza sitios falsos que imitan un portal de noticias de Windows para distribuir un instalador malicioso de la popular herramienta de perfilado del sistema, CPU-Z. El objetivo es engañar a usuarios que buscan CPU-Z en motores de búsqueda como Google, redirigiéndolos a un portal falso (workspace-app[.]online). La campaña forma parte de un patrón más amplio que también ataca otras utilidades como Notepad++, Citrix y VNC Viewer, aprovechando la táctica de crear sitios falsos que imitan a plataformas confiables para atraer a víctimas desprevenidas.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/new-malvertising-campaign-uses-fake.html

---

Nuevo malware Gootloader abusa de RDP para propagarse rápidamente

Investigadores de ciberseguridad de IBM X-Force han identificado un nuevo malware, GootBot, que utiliza el Protocolo de Escritorio Remoto (RDP) para acceso remoto y propagación rápida. En lugar de enfoques convencionales, el grupo Gootloader utiliza SEO poisoning para dirigirse a víctimas y ejecutar el malware, dificultando su detección. GootBot mejora sus capacidades después de la infección, permitiendo a los actores maliciosos permanecer ocultos por más tiempo para ejecutar scripts de PowerShell cifrados. Ambos, GootBot y Gootloader, eran previamente utilizados para obtener acceso inicial a sistemas.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/gootloader-malware-abuses-rdp/

Nuevo Malware para macOS Vinculado a Hackers Norcoreanos

La firma de seguridad Jamf ha identificado un nuevo malware para macOS, llamado ObjCShellz, que se vincula probablemente a hackers norcoreanos dirigidos a intercambios de criptomonedas. Se cree que es parte de la Campaña RustBucket y permite a los atacantes ejecutar instrucciones desde un servidor de control remoto. Aunque la intención precisa no está clara, podría formar parte de futuros ataques de phishing en el sector financiero. Jamf destaca la aparente falta de sofisticación en el malware a pesar de su asociación con un grupo APT norcoreano.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/new-macos-malware-linked-to-north-korean-hackers/

---

37 vulnerabilidades corregidas en Android con las actualizaciones de seguridad de noviembre de 2023

Google ha anunciado parches para 37 vulnerabilidades como parte de las actualizaciones de seguridad de Android de noviembre de 2023, incluyendo una vulnerabilidad crítica de divulgación de información. Los parches abordan problemas en los componentes del sistema y el marco de Android, así como en componentes de Arm, MediaTek y Qualcomm. La vulnerabilidad crítica podría conducir a la divulgación local de información en el componente del sistema. No se ha mencionado que estas vulnerabilidades hayan sido explotadas en ataques maliciosos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.securityweek.com/37-vulnerabilities-patched-in-android-with-november-2023-security-updates/

Servicio Dropper Bypass de Restricciones de Seguridad de Android para Instalar Malware

El servicio dropper recientemente identificado llamado 'SecuriDropper' utiliza una técnica novedosa para eludir las restricciones de seguridad de Android en la entrega de payloads, según informa ThreatFabric, una firma de detección de fraudes en línea. Conocido como Dropper-as-a-Service (DaaS), SecuriDropper utiliza un instalador basado en sesiones para cargar malware, evitando la función de Configuraciones Restringidas que Google introdujo en Android 13. Para sortear las restricciones, SecuriDropper emplea un proceso de infección de dos pasos, distribuyendo una aplicación aparentemente inofensiva que sirve como un dropper para el payload secundario, típicamente malware. SecuriDropper ha sido observado entregando la familia de spyware SpyNote y el troyano bancario Ermac. Este servicio dropper destaca por su capacidad para imitar el proceso de instalación de un mercado, evitando que el sistema operativo identifique el payload como una carga lateral y, por lo tanto, burlando Configuraciones Restringidas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/dropper-service-bypassing-android-security-restrictions-to-install-malware/

Nuevo Grupo de Ransomware "Hunters International" Surge con el Código Fuente e Infraestructura de Hive

El grupo de ransomware "Hunters International" ha adquirido el código fuente e infraestructura de la operación Hive, ya desmantelada, para iniciar sus propias actividades. La transición se percibe como

una estrategia de Hive para cesar operaciones y transferir activos. Hunters International parece centrarse más en la extracción de datos que en el cifrado, y muestra simplificaciones en comparación con Hive, adoptando el código fuente del ransomware basado en Rust. Aunque emergen como un nuevo actor con una herramienta madura, su capacidad y amenaza real están por demostrarse.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/new-ransomware-group-emerges-with-hives.html

---

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

ChatGPT: Riesgos y Beneficios en Ciberseguridad

ChatGPT, se presenta como una herramienta versátil, pero con riesgos de seguridad. Mientras los atacantes pueden emplearlo para encontrar y explotar vulnerabilidades, difundir desinformación o redactar correos de phishing, los defensores pueden aprovecharlo para aprender, analizar informes de seguridad, entender códigos de atacantes y prever rutas de ataque. Se destacan preocupaciones sobre derechos de autor, retención de datos, privacidad, sesgo y la futura capacidad de la IA para identificar textos generados por IA.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/11/offensive-and-defensive-ai-lets-chatgpt.html

---

Ataque de Ransomware al ICBC (Industrial and Commercial Bank of China)

El ICBC ha contenido un ataque de ransomware que afectó el mercado del Tesoro de EE. UU. e impactó algunas transacciones de renta fija y acciones. El ataque, dirigido a ICBC Financial Services, paralizó la liquidación de operaciones del Tesoro, afectando también a algunas transacciones de acciones. Aunque se redirigieron operaciones, el mercado en general continúa operando. La entidad desconectó y aisló los sistemas afectados, iniciando una investigación con expertos externos en ciberseguridad. Se desconoce el grupo de ransomware responsable y si se ha producido robo de datos.

Prioridad: 3 Importante.

Ampliar información:

- https://securityaffairs.com/153986/hacking/icbc-ransomware-attack.html

---

Ciberataque de LockBit a Boeing y Filtración de Datos

El grupo de ransomware LockBit ha publicado datos supuestamente robados del gigante aeroespacial Boeing, añadiéndolo a su lista de víctimas en su sitio de filtraciones en Tor. Alegan haber sustraído una gran cantidad de datos sensibles y amenazan con publicarlos si Boeing no se comunica con ellos antes de la fecha límite. Boeing confirmó que su división de servicios fue atacada y que la investigación está en curso. Se notificó a las autoridades pertinentes, y aunque LockBit afirmó en la web oscura que comenzaría a liberar datos si no se cumplía la demanda de rescate, Boeing se negó a pagar, por lo cual, LockBit filtró más de 40GB de archivos, que según Bleeping Computer, son principalmente copias de seguridad de varios sistemas.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/154115/cyber-crime/lockbit-ransomware-leaked-boeing-data.html#google_vignette

---

WhatsApp presenta la función "Proteger dirección IP en llamadas" para mayor privacidad

WhatsApp, propiedad de Meta, ha lanzado oficialmente una nueva función de privacidad llamada "Proteger dirección IP en llamadas". Esta función enmascara las direcciones IP de los usuarios durante las llamadas al transmitirlas a través de los servidores de WhatsApp, dificultando que los actores malintencionados determinen la ubicación de un usuario. Las llamadas siguen estando cifradas de extremo a extremo, garantizando la privacidad incluso cuando se transmiten a través de los servidores de WhatsApp. Aunque la función mejora la privacidad del usuario, podría haber una ligera disminución en la calidad de las llamadas.

Prioridad: 3 Importante.

Ampliar información:

- https://thehackernews.com/2023/11/whatsapp-introduces-new-privacy-feature.html

---