GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °4723

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

VULNERABILIDADES

Alerta de Zero-Day: Ataque Activo a Google Chrome

Google ha lanzado actualizaciones de seguridad para solucionar siete problemas en su navegador Chrome, incluido un zero-day que está siendo activamente explotado en la naturaleza. Identificado como CVE-2023-6345, se trata de una vulnerabilidad de desbordamiento de entero en Skia, una biblioteca gráfica 2D de código abierto. Descubierto por el Grupo de Análisis de Amenazas (TAG) de Google, se ha confirmado la existencia de un exploit. Es importante señalar que en abril de 2023, Google lanzó parches para un fallo similar en el mismo componente (CVE-2023-2136) que también estaba siendo explotado como zero-day, lo que sugiere que CVE-2023-6345 podría ser un bypass para el primero. En total, Google ha abordado siete zero-days en Chrome desde principios de año, y se recomienda a los usuarios actualizar a la última versión para mitigar posibles amenazas.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/zero-day-alert-google-chrome-under.html?&web_view=true

---

Vulnerabilidades Múltiples en Microsoft Edge

Se han descubierto múltiples vulnerabilidades en Microsoft Edge, que podrían ser explotadas por atacantes remotos para eludir restricciones de seguridad, manipular datos, ejecutar código de forma remota y provocar condiciones de denegación de servicio. Una de las vulnerabilidades, CVE-2023-6345, ha sido identificada como de alto riesgo, con informes de explotación en la naturaleza. Se recomienda a los usuarios que actualicen a las versiones más recientes de Microsoft Edge para mitigar estos riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/microsoft-edge-multiple-vulnerabilities_20231130

Apple Parchea Vulnerabilidades en WebKit Explotadas en iPhones Antiguos

El equipo de respuesta de seguridad de Apple ha lanzado actualizaciones de seguridad para macOS e iOS con el fin de abordar dos fallos graves ya explotados en dispositivos móviles más antiguos. Las vulnerabilidades, identificadas en el motor de navegación WebKit, pueden ser explotadas para secuestrar contenido sensible o realizar ataques de ejecución de código arbitrario. Los exploits pueden ser lanzados a través de contenido web malicioso. Apple insta a los usuarios a actualizar a iOS 17.1.2 o iPadOS 17.1.2 para corregir estos problemas. La empresa reconoce informes de explotación en versiones anteriores a iOS 16.7.1. Las vulnerabilidades también se parchearon en las actualizaciones macOS Sonoma 14.1.2 y Safari 17.1.2.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/apple-patches-webkit-flaws-exploited-on-older-iphones/

Vulnerabilidades en el Kernel de Ubuntu Linux

Se han identificado múltiples vulnerabilidades en productos Ubuntu, abarcando versiones como Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 ESM, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS y Ubuntu 23.04. Un atacante remoto podría aprovechar estas vulnerabilidades para desencadenar denegación de servicio, ejecución remota de código, elevación de privilegios y divulgación de información sensible en los sistemas afectados. Se recomienda a los usuarios aplicar las correcciones proporcionadas por el proveedor para mitigar estos riesgos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.hkcert.org/security-bulletin/ubuntu-linux-kernel-multiple-vulnerabilities_20231201

Zyxel Advierte sobre Vulnerabilidades Críticas en Dispositivos NAS

Zyxel ha corregido múltiples problemas de seguridad en sus dispositivos de almacenamiento en red (NAS), incluyendo tres vulnerabilidades críticas que podrían permitir a un atacante ejecutar comandos en el sistema operativo sin autenticación. Las fallas afectan a los modelos NAS326 y NAS542, y podrían permitir acceso no autorizado, ejecución de comandos y manipulación de datos. Se recomienda a los usuarios que actualicen el firmware a las versiones más recientes para mitigar estos riesgos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/zyxel-warns-of-multiple-critical-vulnerabilities-in-nas-devices/

Vulnerabilidad Crítica en Zoom Permite a Atacantes Tomar el Control de Reuniones

Zoom, la plataforma de videoconferencias más utilizada, ha sido descubierta con una vulnerabilidad crítica que los actores de amenazas podrían potencialmente explotar con diversos fines maliciosos. Esta vulnerabilidad fue informada como parte del evento de hacking H1-4420 llevado a cabo en junio de 2023. Existía en las "Zoom rooms", un sistema desarrollado por Zoom para permitir que los miembros del equipo trabajen juntos desde diferentes ubicaciones a través de Zoom. Un actor de amenazas podría aprovechar esta vulnerabilidad y obtener acceso al inquilino de la organización víctima.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/zoom-vulnerability-take-over-meetings/

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

FjordPhantom, un nuevo malware para Android, utiliza la virtualización para evadir la detección

El nuevo malware para Android, llamado FjordPhantom, utiliza la virtualización para ejecutar código malicioso en un contenedor, evadiendo la detección. Se propaga a través de diversos medios y apunta a aplicaciones bancarias en el sudeste asiático. FjordPhantom busca robar credenciales bancarias y realizar fraudes en el dispositivo, aprovechando técnicas de ingeniería social. Su ataque de virtualización elude el concepto de seguridad de 'Android Sandbox'. Este malware está en desarrollo activo, aumentando el riesgo de una expansión futura.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/fjordphantom-android-malware-uses-virtualization-to-evade-detection/#google_vignette

Hackers Utilizan la Herramienta ScrubCrypt para Evadir Antivirus y Desplegar el Malware RedLine

La herramienta de ofuscación ScrubCrypt ha sido empleada por hackers en ataques para distribuir el malware RedLine Stealer, con su nueva variante activamente promocionada en foros clandestinos. ScrubCrypt ayuda a los actores de amenazas a eludir la detección antivirus, permitiéndoles ejecutar ataques que de otro modo podrían ser frustrados. RedLine Stealer es conocido por exfiltrar billeteras y credenciales de criptomonedas, apuntando a usuarios a través de la usurpación de cuentas y fraudes. El uso de archivos por lotes en la nueva versión de ScrubCrypt permite a los actores de amenazas eludir medidas preventivas y evadir la detección antivirus.

Prioridad: 1 Crítico.

Ampliar información:

- https://gbhackers.com/hackers-antivirus-redline-malware/#google_vignette

---

LogoFAIL: Inyección Sigilosa de Bootkits a través de Logotipos de Arranque UEFI

Las vulnerabilidades LogoFAIL en componentes de análisis de imágenes de código UEFI pueden ser explotadas para inyectar bootkits durante el proceso de arranque, advierten investigadores de Binarly. Al afectar las bibliotecas de análisis de imágenes utilizadas para mostrar logotipos, estas vulnerabilidades representan un riesgo generalizado para arquitecturas x86 y ARM. La ejecución de cargas maliciosas es posible al inyectar archivos de imagen en la Partición del Sistema EFI. LogoFAIL no requiere modificar el cargador de arranque o el firmware, lo que lo hace especialmente sigiloso y persistente en el sistema. La extensión exacta del impacto aún se está determinando, pero cientos de dispositivos de múltiples fabricantes podrían ser vulnerables. Detalles técnicos adicionales se presentarán en la conferencia Black Hat Europe el 6 de diciembre.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/logofail-attack-can-install-uefi-bootkits-through-bootup-logos/

Un avanzado ransomware Linux de la banda Qilin se centra en VMware ESXi

Un cifrador de la banda de ransomware Qilin, diseñado para Linux, ha sido descubierto y podría ser uno de los más avanzados y personalizables vistos hasta la fecha. Este cifrador se centra especialmente en las máquinas virtuales VMware ESXi, utilizadas cada vez más por las empresas para alojar servidores. A diferencia de otros que utilizan código fuente filtrado, Qilin desarrolla su propio cifrador para atacar servidores Linux. El cifrador de Qilin permite una personalización extensa, enfocándose en cifrar máquinas virtuales y eliminar sus instantáneas. Las exclusiones y criterios de destino se pueden configurar, y la detección de VMware ESXi desencadena comandos específicos para este entorno. La operación de ransomware Qilin, activa desde agosto de 2022, ha demostrado ser una amenaza persistente, utilizando tácticas de doble extorsión y dirigiéndose a empresas con creciente actividad a finales de 2023.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/linux-version-of-qilin-ransomware-focuses-on-vmware-esxi/#google_vignette

---

Nuevo malware proxy ataca a usuarios de Mac a través de software pirateado

Ciberdelincuentes están utilizando un nuevo malware proxy para dirigirse a usuarios de Mac, aprovechándose de versiones pirateadas de software macOS popular. El troyano proxy infecta computadoras y las convierte en terminales de reenvío de tráfico, utilizadas para actividades maliciosas como hacking y phishing. El ataque, descubierto por Kaspersky, se disfraza entre software con derechos de autor ofrecido en sitios de warez, atrayendo a aquellos que buscan versiones gratuitas de aplicaciones premium.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-proxy-malware-targets-mac-users-through-pirated-software/

Nuevo ransomware amenaza a usuarios de MAC

Se ha identificado un nuevo ransomware llamado Turtle dirigido a dispositivos con macOS. Aunque su nivel de sofisticación es limitado, el malware representa una amenaza potencial al cifrar archivos mediante AES. La detección por parte de múltiples soluciones antivirus sugiere un aumento en la actividad de ransomware dirigido a la plataforma macOS, lo que destaca la importancia de la vigilancia y las precauciones de seguridad por parte de los usuarios de Mac.

Prioridad: 3 Importante.

Ampliar información:

- https://securityaffairs.com/155075/security/turtleransom-macos-ransomware.html?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.

NOTICIAS DE CIBERSEGURIDAD

Nuevo Ataque BLUFFS Permite a Atacantes Secuestrar Conexiones Bluetooth

Investigadores de Eurecom descubrieron seis ataques denominados colectivamente 'BLUFFS' que comprometen la confidencialidad de las sesiones de Bluetooth. Estos exploits aprovechan fallas en el estándar de Bluetooth, afectando miles de millones de dispositivos. BLUFFS apunta a romper la confidencialidad de las comunicaciones pasadas y futuras, forzando la derivación de claves de sesión débiles y predecibles. Los investigadores proporcionaron herramientas en GitHub para demostrar estos ataques y sugieren modificaciones para mitigar la amenaza. Las vulnerabilidades afectan Bluetooth 4.2 hasta 5.4.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-bluffs-attack-lets-attackers-hijack-bluetooth-connections/#google_vignette

---

Vulnerabilidad en ChatGPT Revela Riesgo de Extracción de Datos Personales

Investigadores de seguridad de Google han demostrado la vulnerabilidad de ChatGPT al extraer datos de entrenamiento memorizados mediante consultas específicas, con un costo de solo 250 euros. Utilizando técnicas de "prompt hacking", lograron forzar a la IA a revelar información sensible. Aunque grandes empresas como OpenAI y Google trabajan en parches.

Prioridad: 3 Importante.

Ampliar información:

- https://www.genbeta.com/actualidad/han-conseguido-enganar-a-chatgpt-filtre-datos-personales-investigadores-google-se-han-alarmado-resultado

---

Hackers Utilizan Credenciales Robadas de Booking.com para Estafar a Huéspedes de Hoteles

Un sofisticado ataque de phishing dirigido a hoteles y sus clientes se llevó a cabo mediante la popular plataforma Booking.com, según un informe reciente de Secureworks. Los atacantes utilizaron una campaña de phishing avanzada para engañar a las víctimas y obtener su información personal, incluidos los datos de pago. El ataque destaca la creciente amenaza del cibercrimen en la industria hotelera y la necesidad de medidas de seguridad más sólidas para proteger los datos sensibles de los clientes. Los atacantes emplearon el stealer de información Vidar para robar credenciales de Booking.com de personal hotelero, demostrando la creciente demanda de estos datos en foros clandestinos.

Prioridad: 2 Urgente.

Ampliar información:

- https://gbhackers.com/hotels-hacked-logins/
