GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °5023

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	4	
MALWARE	1	1	2
NOTICIAS DE CIBERSEGURIDAD	1	1	2

VULNERABILIDADES

ESET resuelve vulnerabilidad en función de escaneo de tráfico seguro

ESET ha corregido una vulnerabilidad crítica (CVE-2023-5594, CVSS 7.5) en su Función de Escaneo de Tráfico Seguro, evitando la posibilidad de que los navegadores confíen en sitios web con certificados anticuados. La falla, relacionada con la validación incorrecta de la cadena de certificados del servidor, afectó a varios productos de ESET, incluyendo NOD32 Antivirus y Smart Security Premium. Aunque no se han reportado ataques, se insta a los usuarios a actualizar a través del módulo de protección de Internet 1464, distribuido automáticamente.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/156256/security/eset-secure-traffic-scanning-feature-bugs.html?web_view=true

---

Ivanti parchea 13 vulnerabilidades críticas en Avalanche MDM

Ivanti ha lanzado actualizaciones para abordar 13 vulnerabilidades críticas en su solución de gestión de dispositivos móviles Avalanche. Las debilidades, descubiertas por investigadores de Tenable y Zero Day Initiative de Trend Micro, incluyen desbordamientos de búfer en WLAvalancheService, permitiendo a atacantes no autenticados lograr ejecución remota de código sin interacción del usuario. La compañía recomienda la actualización a Avalanche 6.4.2 para mitigar los riesgos, afectando a todas las versiones compatibles, desde la 6.3.1 en adelante. También se han corregido ocho vulnerabilidades de severidad media y alta que podrían ser explotadas para ataques de denegación de servicio y ejecución remota de código.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/ivanti-releases-patches-for-13-critical-avalanche-rce-flaws/?&web_view=true#google_vignette

---

Google aborda con urgencia una nueva vulnerabilidad zero-day en Chrome

Google ha lanzado actualizaciones de emergencia para resolver una vulnerabilidad zero-day, identificada como CVE-2023-7024, en su navegador Chrome. Esta falla crítica, un desbordamiento de búfer en la Heap de WebRTC, fue informada por el Grupo de Análisis de Amenazas de Google y solucionada en un día. La empresa advierte que existe un exploit en la naturaleza para esta vulnerabilidad, sugiriendo una posible explotación por actores estatales o firmas de vigilancia. Esta es la octava vulnerabilidad zero-day abordada por Google en lo que va del año, subrayando la importancia de mantener los navegadores actualizados para mitigar riesgos de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://securityaffairs.com/156231/security/google-addressed-a-new-actively-exploited-chrome-zero-day.html?web_view=true

---

Apple lanza iOS 17.2 con parches de seguridad urgentes

Apple ha lanzado iOS 17.2 y iPadOS 17.2 con correcciones para al menos 11 vulnerabilidades de seguridad, algunas de las cuales podrían llevar a la ejecución de código arbitrario o a la fuga del sandbox de la aplicación. Las vulnerabilidades abordadas incluyen problemas de corrupción de memoria en ImageIO, ejecución de código en el motor de renderizado WebKit y problemas de seguridad en la memoria. Apple también ha lanzado iOS 16.7.3 y iPadOS 16.7.3 para dispositivos que ejecutan versiones más antiguas del sistema operativo, que incluyen correcciones para problemas previamente documentados en WebKit.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/156231/security/google-addressed-a-new-actively-exploited-chrome-zero-day.html?web_view=true

---

CISA advierte sobre vulnerabilidades explotadas en routers FXC y dispositivos QNAP NVR

La agencia de ciberseguridad de EE. UU., CISA, alerta sobre vulnerabilidades en routers de Future X Communications y dispositivos de grabación de video QNAP, explotadas en la naturaleza. Ambas presentan riesgo de ejecución remota de código. FXC y QNAP lanzaron parches, pero es esencial actuar rápidamente. Las vulnerabilidades se han aprovechado en campañas conocidas como "InfectedSlurs", según informes de Akamai. Aunque se requiere autenticación para explotarlas, los ciberdelincuentes confían en contraseñas predeterminadas no cambiadas por los usuarios.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/cisa-warns-of-fxc-router-qnap-nvr-vulnerabilities-exploited-in-the-wild/

Mozilla parchea vulnerabilidad en Firefox que permite la ejecución remota de código y la evasión del contenedor de seguridad

Mozilla ha lanzado actualizaciones de seguridad para Firefox y Thunderbird, abordando 20 vulnerabilidades, incluidos varios problemas de seguridad de la memoria. La versión 121 de Firefox resuelve 18 vulnerabilidades, destacando CVE-2023-6856, una falla crítica de desbordamiento de búfer en WebGL que podría permitir a un atacante la ejecución remota de código y la evasión del contenedor de seguridad. Otras correcciones incluyen problemas de seguridad de la memoria, escapes de contenedor y desbordamientos de búfer.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/mozilla-patches-firefox-vulnerability-allowing-remote-code-execution-sandbox-escape/

Outlook: elusiones de parches para vulnerabilidad de ejecución remota de código sin clics

Akamai ha identificado múltiples elusiones para los parches lanzados por Microsoft para una vulnerabilidad de ejecución remota de código en Outlook (CVE-2023-23397). La original, solucionada en marzo, permitía a un atacante no autenticado explotarla enviando un recordatorio de correo electrónico con una notificación de sonido como ruta, conectando al cliente Outlook al

servidor del atacante, enviando el hash Net-NTLMv2 al servidor. Akamai descubrió un bypass (CVE-2023-29324) en mayo, donde la función de la API podía ser engañada con una URL manipulada. Dos elusiones adicionales (CVE-2023-35384 y CVE-2023-36710) fueron abordadas en agosto y octubre. La primera es una confusión de tipo de ruta que requiere interacción del usuario; la segunda es un desbordamiento de enteros en Audio Compression Manager.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/outlook-plays-attacker-tunes-vulnerability-chain-leading-to-zero-click-rce/

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

Chameleon Banking Trojan: avances en evasión biométrica

El Chameleon Banking Trojan, detectado por primera vez a principios de 2023, ha resurgido con una variante mejorada que ahora puede sortear cualquier autenticación biométrica en dispositivos Android. Esta versión evolucionada es distribuida a través de Zombinder. Dos características destacadas incluyen la capacidad de eludir solicitudes biométricas y mostrar una página HTML para habilitar el servicio de accesibilidad en dispositivos con Android 13. Estas nuevas capacidades reflejan la adaptabilidad y sofisticación del Chameleon, subrayando su amenaza continua en el panorama de seguridad móvil.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action?&web_view=true

---

Nuevo malware JaskaGO amenaza sistemas Windows y macOS

El malware, identificado por primera vez en julio de 2023 en instaladores de software pirateado, muestra una baja tasa de detección. Después de la ejecución inicial, JaskaGO realiza comprobaciones para evitar operar en entornos virtualizados y recopila información del sistema infectado, enviándola a su infraestructura de comando y control. El malware es capaz de mantener persistencia, ejecutar comandos shell, robar información del navegador y realizar diversas acciones, destacando su peligrosidad y habilidad para eludir la detección.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/156185/malware/jaskago-information-stealer-macos-windows.html

---

Hackers aprovechan vulnerabilidad antigua en Microsoft Office para desplegar malware

Malwares como Agent Tesla están siendo utilizados por ciberdelincuentes para atacar usuarios de Microsoft Office que aún utilizan versiones afectadas por CVE-2017-11882 XLAM. Esta vulnerabilidad, presente en Equation Editor de Microsoft Office, permite la ejecución remota de código (RCE). Cuando un usuario abre un archivo malicioso en Excel, se inicia la descarga de otros archivos sin necesidad de interacción adicional. Agent Tesla, una vez activado, monitorea las pulsaciones de teclas y recopila datos sensibles, enviándolos al atacante a través de un bot de Telegram.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/hackers-exploiting-old-microsoft-office-rce-flaw/#google_vignette

---

Nuevos descargadores de OilRig abusan de las Apis en la nube de Microsoft para comunicaciones de C&C

El grupo de ciberespionaje OilRig, activo desde 2014 y enfocado en gobiernos del Medio Oriente, está utilizando nuevos descargadores que abusan de las APIs en la nube de Microsoft para comunicaciones de C&C (comando y control). Estos descargadores, como ODAgent, están diseñados para descargar, ejecutar y extraer archivos, se dirigen a objetivos específicos, especialmente en entornos de Office 365. OilRig ha evolucionado a lo largo de los años, utilizando tácticas avanzadas para ocultar sus actividades maliciosas, adaptándose a nuevas infraestructuras, como el uso de servicios en la nube de Microsoft para sus comunicaciones C&C. Esta estrategia refleja la continua evolución de los actores de amenazas para eludir la detección y mantener la eficacia en sus operaciones de ciberespionaje.

Prioridad: 3 Importante.

Ampliar información:

- https://gbhackers.com/new-oilrig-downloaders-abusing-microsoft/

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

Ataque de phishing a usuarios de Instagram expone códigos de respaldo de 2FA

En un nuevo ataque de phishing, los ciberdelincuentes se hacen pasar por mensajes de 'infracción de derechos de autor' para robar códigos de respaldo de Instagram. Al simular ser correos de Meta, la empresa matriz de Instagram, los estafadores instan a los usuarios a hacer clic en enlaces que

los llevan a páginas de phishing. Una vez allí, los usuarios ingresan sus credenciales y, posteriormente, se les solicita el código de respaldo de 8 dígitos de la autenticación de dos factores (2FA). Aunque la estafa presenta señales de fraude, el diseño convincente y la urgencia pueden engañar a usuarios desprevenidos, subrayando la importancia de mantener la privacidad de los códigos de respaldo.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/new-phishing-attack-steals-your-instagram-backup-codes-to-bypass-2fa/?&web_view=true/

Informe de seguridad Microsoft Digital Defense 2023

El informe de seguridad de Microsoft Digital Defense 2023 destaca el aumento significativo de los ataques de ransomware operados por humanos y el drástico incremento en los ataques basados en contraseñas. Además, señala un récord en los intentos diarios de compromiso de correo electrónico empresarial (BEC) y la expansión de amenazas de estados-nación. Destaca la importancia crítica de la inteligencia artificial (IA) y los grandes modelos de lenguaje para fortalecer las defensas cibernéticas, pero subraya la necesidad de precauciones para garantizar la responsabilidad y la privacidad.

Prioridad: 3 Importante.

Ampliar información:

- https://www.darkreading.com/threat-intelligence/5-essential-insights-from-the-microsoft-digital-defense-report-2023

"Wall of Flippers": detectando ataques de spam Bluetooth de Flipper Zero y Android

El proyecto "Wall of Flippers" es una nueva iniciativa en Python que detecta ataques de spam Bluetooth lanzados por dispositivos Flipper Zero y Android. Este proyecto permite a los usuarios detectar estos ataques y conocer su origen, lo que facilita la toma de medidas de protección específicas. La herramienta identifica las amenazas, registrando información clave, como la dirección MAC del dispositivo atacante, la potencia de la señal o los datos contenidos en los paquetes transmitidos. Esta capacidad es crucial, ya que los ataques Bluetooth spam pueden tener consecuencias más allá de bromas inofensivas, afectando dispositivos médicos. causando interrupciones en servicios comerciales. La herramienta está diseñada para ejecutarse continuamente y proporcionar actualizaciones sobre la actividad de dispositivos Bluetooth cercanos, ayudando a los usuarios a tomar medidas adecuadas.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/wall-of-flippers-detects-flipper-zero-bluetooth-spam-attacks/

Bluesnarfing: amenaza a través de Bluetooth

El "Bluesnarfing", una ciberestafa que explota vulnerabilidades en la tecnología Bluetooth, ha sido señalada como un riesgo por el Banco de España. Este ataque activo permite a los hackers robar datos bancarios y personales almacenados en dispositivos dentro de un radio de 10-15 metros. Para prevenirlo, se aconseja mantener el firmware actualizado, configurar Bluetooth en modo "no visible", desactivarlo cuando no se use y usar contraseñas fuertes.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.genbeta.com/seguridad/que-bluesnarfing-nueva-ciberestafa-que-te-roba-datos-a-traves-tus-dispositivos-bluetooth

---