GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º4323

BOLETIN 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		2	3
NOTICIAS DE CIBERSEGURIDAD	1	1	2

VULNERABILIDADES

QNAP advierte sobre vulnerabilidades críticas de inyección de comandos en QTS OS y aplicaciones

QNAP Systems ha emitido advertencias de seguridad por dos vulnerabilidades críticas de inyección de comandos que afectan a múltiples versiones del sistema operativo QTS y aplicaciones en sus dispositivos NAS. La primera vulnerabilidad, con un nivel de gravedad de 9.8, permite a un atacante remoto ejecutar comandos a través de la red. La segunda vulnerabilidad, con una gravedad de 9.0, también es explotable por atacantes remotos. Se recomienda a los usuarios de QNAP aplicar las actualizaciones de seguridad disponibles de inmediato.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/qnap-warns-of-critical-command-injection-flaws-in-qts-os-apps/?&web_view=true#google_vignette

---

Trend Micro Zero Day Initiative Expone Cuatro Vulnerabilidades Zero-Day en Microsoft Exchange

Trend Micro Zero Day Initiative (ZDI) ha revelado cuatro vulnerabilidades zero-day en Microsoft Exchange que permiten la ejecución remota de código o la divulgación de información sensible. A pesar de la notificación a Microsoft, las vulnerabilidades aún no han sido parcheadas. Estas vulnerabilidades fueron descubiertas por Piotr Bazydlo de Trend Micro Zero Day Initiative.

Prioridad: 1 Crítico.

Ampliar información:

- https://securityaffairs.com/153599/hacking/microsoft-exchange-zero-day-flaws.html?web_view=true/

Cisco Publica Actualizaciones para Resolver 27 Vulnerabilidades en Productos de Seguridad de Red

Cisco ha lanzado actualizaciones de software para abordar 27 vulnerabilidades en sus productos Adaptive Security Appliance (ASA), Firepower Management Center (FMC) y Firepower Threat Defense (FTD). Estas actualizaciones incluyen correcciones para problemas de alta, media y baja gravedad, con la vulnerabilidad más grave: CVE-2023-20048, que permite la inyección de comandos en FMC, además, tiene un puntaje CVSS de 9.9. Cisco ha publicado siete avisos detallando ocho problemas de alta gravedad y 18 de gravedad media. A pesar de la disponibilidad pública de códigos de explotación de prueba de concepto (PoC) para algunas de estas vulnerabilidades, Cisco no tiene conocimiento de ataques en la naturaleza que aprovechen estas vulnerabilidades.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.securityweek.com/cisco-patches-27-vulnerabilities-in-network-security-products/?web_view=true/

Vulnerabilidad Zero-Day de Apache ActiveMQ Explotada Dos Semanas Antes de la Publicación de Parches

La vulnerabilidad CVE-2023-46604 de Apache ActiveMQ fue explotada maliciosamente como zero-day desde al menos el 10 de octubre, dos semanas antes de que se lanzaran parches. Aunque se intentó la explotación, la infección no tuvo éxito. La vulnerabilidad es fácil de explotar y se recomienda que los usuarios actualicen a las versiones parcheadas lo antes posible.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/apache-activemq-vulnerability-exploited-as-zero-day/

'Citrix Bleed' en NetScaler ADC y Gateway (CVE-2023-4966)

Explotación masiva de la vulnerabilidad 'Citrix Bleed' en curso en NetScaler ADC y Gateway (CVE-2023-4966). Investigadores de seguridad advierten que varios actores de amenazas están explotando esta vulnerabilidad crítica que permite el secuestro de sesiones. Se han aplicado parches, pero muchas instancias siguen siendo vulnerables. Se recomienda a las organizaciones que apliquen los parches y eliminen las sesiones activas o persistentes para abordar el problema.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.securityweek.com/mass-exploitation-of-citrix-bleed-vulnerability-underway/

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

SecuriDropper: nuevo servicio de instalación de malware para Android burla las defensas de Google

Investigadores de ciberseguridad han revelado SecuriDropper, un servicio de instalación de malware para Android que elude las restricciones de seguridad de Google y facilita la entrega de programas maliciosos. Este enfoque permite a los atacantes separar el desarrollo y la ejecución de un ataque de la instalación del malware, lo que representa un desafío para las medidas de seguridad en constante evolución de Android.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/securidropper-new-android-dropper-as.html?&web_view=true

---

Nueva Versión del Backdoor Kazuar

El grupo de piratería Turla, vinculado a Rusia, ha sido observado utilizando una nueva versión del backdoor Kazuar para expandir sus ataques. La nueva variante de Kazuar admite más de 40 comandos previamente no documentados, lo que permite a los atacantes robar datos, capturar pantallas, obtener información del sistema y ejecutar scripts. Esta actualización demuestra los esfuerzos constantes de Turla APT por operar de manera sigilosa y sofisticada. Organizaciones deben estar alerta para detectar y bloquear amenazas dirigidas a sus activos críticos e infraestructuras.

Prioridad: 3 Importante.

Ampliar información:

- https://cyware.com/news/researchers-uncover-a-new-version-of-kazuar-backdoor-24c45eaf/?web_view=true/

Ciberdelincuentes intensifican los ataques a través de archivos XLL habilitados para macros

Ciberdelincuentes están utilizando cada vez más archivos XLL habilitados para macros en ataques de malware, según un informe de HP Wolf Security. Estos archivos se han vuelto más comunes en los ataques, ofreciendo a los atacantes mayor capacidad y evitando las restricciones de Microsoft en las macros de Visual Basic for Applications (VBA). Los atacantes utilizan estos archivos para entregar malware directamente en documentos de Microsoft Office, lo que subraya la importancia de mantener la seguridad en los entornos empresariales.

Prioridad: 3 Importante.

Ampliar información:

- https://www.theregister.com/2023/11/01/xll_macro_attack_surge/?&web_view=true

---

Kits de Malware 'Meal Kits' Facilitan Ataques RAT

Los "kits de comida" de malware, disponibles por menos de $100, están impulsando una oleada de campañas de acceso remoto con troyanos (RATs) que a menudo se encuentran en archivos de Excel y PowerPoint aparentemente legítimos adjuntos a correos electrónicos. Los kits de malware de Parallax RAT están disponibles por $65 al mes en foros de hacking, y los atacantes parecen estar aprovechando a otros atacantes menos experimentados en algunas campañas de RAT.

Prioridad: 3 Importante.

Ampliar información:

- https://www.darkreading.com/endpoint/malware-meal-kits-serve-up-no-fuss-rat-attacks?&web_view=true

---

Múltiples mods de WhatsApp descubiertos que contienen el spyware CanesSpy

Kaspersky advierte sobre mods de WhatsApp que contienen el troyano CanesSpy y se distribuyen a través de canales de Telegram, principalmente en árabe y azerí. El malware recopila información del dispositivo y se comunica con un servidor de control. Los países más afectados son Azerbaiyán, Arabia Saudita, Yemen, Turquía y Egipto. Kaspersky recomienda usar solo clientes oficiales de mensajería.

Prioridad: 2 Urgente.

Ampliar información:

- https://securityaffairs.com/153564/mobile-2/whatsapp-mods-canesspy-spyware.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

Google Advierte Sobre el Abuso de Google Calendar para Comandos Encubiertos

Google ha emitido una advertencia sobre amenazas de un exploit de prueba de concepto (PoC) que utiliza Google Calendar para alojar una infraestructura de control y comando (C2). La herramienta, denominada Google Calendar RAT (GCR), emplea eventos del Calendario de Google para C2 a través de una cuenta de Gmail. Aunque Google no ha visto el uso de esta herramienta en la naturaleza, su unidad de inteligencia de amenazas Mandiant ha detectado a varios actores compartiendo el PoC en foros clandestinos. El GCR permite a un dispositivo comprometido realizar comandos a través de Google Calendar, lo que hace que la detección de actividad sospechosa sea difícil debido a que opera en infraestructura legítima.

Prioridad: 2 Urgente.

Ampliar información:

- https://thehackernews.com/2023/11/google-warns-of-hackers-absing-calendar.html?&web_view=true

---

Socks5Systemz: Botnet de Proxy Infecta 10,000 Sistemas en Todo el Mundo

Un botnet de proxy llamado 'Socks5Systemz' ha infectado 10,000 sistemas en todo el mundo mediante los cargadores de malware 'PrivateLoader' y 'Amadey', convirtiendo las computadoras en proxies para tráfico malicioso o anónimo. Este servicio se vende a suscriptores que pagan entre $1 y $140 al día en criptomonedas. Socks5Systemz ha estado operando desde al menos 2016 y ha permanecido relativamente desconocido hasta ahora, pero su impacto en la seguridad de Internet es significativo.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/socks5systemz-proxy-service-infects-10-000-systems-worldwide/?&web_view=true#google_vignette

---

Abuso del Servicio 'Find My' de Apple para Robar Contraseñas Registradas por Keyloggers

El servicio "Find My" de Apple puede ser utilizado por actores maliciosos para transmitir información sensible capturada por keyloggers en teclados a través de la red Bluetooth. Investigadores de Positive Security han demostrado que es posible aprovechar esta función para enviar contraseñas y otros datos confidenciales a través de dispositivos Apple en todo el mundo. Aunque el proceso es lento, esta vulnerabilidad podría ser explotada para recuperar información valiosa sin activar las

protecciones de seguimiento de Apple. Hasta el momento, Apple no ha respondido a estas preocupaciones.

Prioridad: 3 Importante.

Ampliar información:

- https://www.bleepingcomputer.com/news/apple/apple-find-my-network-can-be-abused-to-steal-keylogged-passwords/?&web_view=true

---

Actores de Kinsing Explotan Falla Reciente en Linux para Infiltrar Entornos en la Nube

Actores vinculados a Kinsing intentan explotar la reciente falla de Linux llamada Looney Tunables en una nueva campaña para infiltrar entornos en la nube. Esta es la primera instancia pública de explotación activa de esta vulnerabilidad, lo que representa un cambio táctico en el comportamiento de Kinsing, ya que ahora buscan extraer credenciales del proveedor de servicios en la nube, ampliando su amenaza a los entornos nativos de la misma.

Prioridad: 1 Crítico.

Ampliar información:

- https://thehackernews.com/2023/11/kinsing-actors-exploit-linux-flaw-to.html?&web_view=true/
