GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición °0925

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	0	3	0
MALWARE	0	0	2
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Explotan vulnerabilidad en Krpano para inyectar anuncios de spam en más de 350 sitios web

Investigadores de seguridad han identificado una campaña maliciosa, denominada 360XSS, que afecta a más de 350 sitios web, incluyendo portales gubernamentales, universidades, cadenas hoteleras y empresas. El actor implicado en esta campaña es un grupo de ciberdelincuentes que explotan una vulnerabilidad de tipo cross-site scripting (XSS) en el framework Krpano, utilizado para incrustar imágenes y videos de 360° en experiencias de realidad virtual. Esta nueva aparición de la vulnerabilidad, fue descubierta y se adjuntó estos nuevos descubrimientos a la ya catalogada como CVE-2020-24901 con una puntuación CVSS de 6.1, la cual permite a los atacantes inyectar scripts maliciosos en sitios web legítimos, manipulando los resultados de búsqueda para promover anuncios de spam relacionados con pornografía, suplementos dietéticos y casinos en línea.

La explotación se basa en la configuración "passQueryParameters" de Krpano, que, si está habilitada, permite a los atacantes ejecutar scripts maliciosos a través de URLs especialmente diseñadas. Aunque la versión 1.20.10 de Krpano introdujo restricciones para mitigar este riesgo, configuraciones específicas que incluyen el parámetro XML pueden reintroducir la vulnerabilidad. Se recomienda a los usuarios de Krpano actualizar a la versión más reciente y deshabilitar la opción "passQueryParameters" para evitar posibles ataques. Los propietarios de sitios web afectados deben revisar y eliminar páginas infectadas utilizando herramientas como Google Search Console, entre otras.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/hackers-exploited-krpano-framework-flaw.html

---

PolarEdge: Botnet que explota vulnerabilidades en dispositivos de Cisco, ASUS, QNAP y Synology

Un nuevo malware, denominado PolarEdge, ha sido identificado apuntando a dispositivos de borde de marcas como Cisco, ASUS, QNAP y Synology desde finales de 2023 hasta los más recientes descubrimientos en 2025. Investigadores de la empresa de ciberseguridad Sekoia descubrieron que actores desconocidos están aprovechando la vulnerabilidad CVE-2023-20118 (con una puntuación CVSS de 6.5) en routers Cisco Small Business RV016, RV042, RV042G, RV082, RV320 y RV325. Esta vulnerabilidad permite la ejecución arbitraria de comandos en dispositivos afectados y permanece sin parchear debido a que estos routers han alcanzado su estado de fin de vida útil

La explotación de esta vulnerabilidad implica la entrega de un implante no documentado previamente: una puerta trasera TLS que escucha conexiones entrantes y ejecuta comandos. Este denominado PolarEdge, establece un bucle infinito para mantener una sesión TLS y gestionar solicitudes del cliente, permitiendo a los atacantes ejecutar

comandos en los dispositivos comprometidos. Hasta ahora, se estima que el Botnet ha comprometido 2,017 direcciones IP únicas en todo el mundo, con infecciones predominantes en Estados Unidos, Taiwán, Rusia, India, Brasil, Australia y Argentina. Para mitigar este riesgo, se recomienda deshabilitar la gestión remota y bloquear el acceso a los puertos 443 y 60443 en los dispositivos afectados, según las directrices proporcionadas por Cisco.

Prioridad: Urgente.

Ampliar Información:

https://thehackernews.com/2025/02/polaredge-botnet-exploits-cisco-and.html

---

Cisco soluciona vulnerabilidades en switches Nexus

Cisco ha lanzado actualizaciones de seguridad para abordar varias vulnerabilidades en sus switches Nexus, incluyendo una de alta severidad. La vulnerabilidad más crítica, identificada como CVE-2025-20111, la cual afecta a los componentes de diagnóstico de salud de los switches Nexus 3000 y 9000 series. Esta falla se debe al manejo incorrecto de ciertos tramas Ethernet, lo que permite a un atacante no autenticado con acceso al dispositivo provocar una condición de denegación de servicio (DoS) al enviar una tasa sostenida de tramas Ethernet especialmente diseñadas, causando que el dispositivo se reinicie.

Además, se identificó una vulnerabilidad de severidad media en los mismos modelos de switches Nexus, que permite a un atacante local con credenciales de administrador ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios de root al instalar una imagen manipulada. Para mitigar estos riesgos, Cisco recomienda encarecidamente a los administradores de sistemas que actualicen sus dispositivos Nexus a las versiones de software que corrigen estas vulnerabilidades. La empresa no tiene conocimiento de que estas fallas hayan sido explotadas activamente en entornos reales

hasta la fecha, pero no se descarta debido a su riesgo su posible aparición en América Latina

Prioridad: Urgente.

Ampliar Información:

https://www.securityweek.com/cisco-patches-vulnerabilities-in-nexus-switches/

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.

2. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.

3. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.

4. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.

5. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Nuevo malware 'Auto-Color' compromete sistemas Linux con acceso remoto total

Investigadores de Unit 42 de Palo Alto Networks han identificado un nuevo malware denominado 'Auto-Color', dirigido a sistemas Linux en universidades y agencias gubernamentales, se podría despegar y afectar todos los países que tengas estos sistemas, Se cree que el ataque proviene de un grupo APT (Advanced Persistent Threat),

cuyo objetivo es obtener acceso persistente y no autorizado a los sistemas afectados. Este malware se propaga a través de la ejecución manual de archivos disfrazados de software legítimo, aprovechando la falta de medidas de seguridad adecuadas en servidores mal configurados.

'Auto-Color' es un malware sofisticado que emplea técnicas avanzadas de evasión. Una vez ejecutado, instala una biblioteca maliciosa ('libcext.so.2'), se oculta en /var/log/cross/auto-color, y modifica el archivo /etc/ld.preload para garantizar su persistencia en el sistema. Además, cifra su comunicación con los servidores de comando y control (C2), dificultando su detección. Para protegerse, los expertos recomiendan evitar ejecutar archivos de fuentes desconocidas, monitorear cambios en /etc/ld.preload, utilizar soluciones de seguridad avanzadas y mantener los sistemas actualizados.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/02/new-linux-malware-auto-color-grants.html

---

Campaña Masiva de PDFs maliciosos para distribuir malware Lumma Stealer

Investigadores de Netskope Threat Labs han identificado una campaña masiva de phishing que utiliza más de 5,000 archivos PDF maliciosos alojados en 260 dominios para distribuir el malware Lumma Stealer. Los atacantes han utilizado técnicas de SEO malicioso para hacer que estos documentos aparezcan en los resultados de búsqueda y engañar a las víctimas. Los PDFs contienen imágenes de CAPTCHAs falsos, que al ser interactuados redirigen a las víctimas a sitios web controlados por los atacantes, donde se ejecutan scripts de PowerShell que terminan instalando el malware. Esta campaña ha afectado a más de 1,150 organizaciones y 7,000 usuarios, principalmente en América del Norte, Asia y el sur de Europa, aunque no se descarta su paso por Latinoamérica, Esto con un enfoque en los sectores de tecnología, finanzas y manufactura.

El malware Lumma Stealer, identificado como un stealer-as-a-service, es capaz de robar credenciales, datos financieros y otra información sensible de sistemas Windows comprometidos. En versiones recientes, ha integrado compatibilidad con GhostSocks, un proxy basado en Golang que permite a los atacantes evadir restricciones geográficas y detecciones basadas en IP. Se recomienda a los usuarios evitar abrir PDFs de fuentes desconocidas, implementar soluciones de seguridad actualizadas, bloquear la ejecución de scripts sospechosos en entornos corporativos y capacitar a los empleados para reconocer intentos de phishing sofisticados.

Prioridad: Importante.

Ampliar Información:

https://thehackernews.com/2025/02/5000-phishing-pdfs-on-260-domains.html

---

Recomendaciones generales sobre Malware

Para protegerse contra malware, es esencial:

- Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
- Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
- Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
- Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
- Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
- Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Mozilla ajusta términos de uso de Firefox tras críticas sobre privacidad de datos

Mozilla ha actualizado nuevamente los términos de uso de Firefox después de recibir críticas por el lenguaje amplio utilizado en su política de licencia de datos. La versión original, introducida el 26 de febrero, indicaba que los usuarios otorgaban a Mozilla una licencia mundial, libre de regalías y no exclusiva para usar la información ingresada en el navegador, lo que generó preocupaciones sobre el acceso y control de los datos personales. La controversia fue identificada por la comunidad de usuarios y expertos en privacidad, quienes señalaron que la redacción sugería que Mozilla podría recolectar información más allá de lo necesario. En respuesta, la compañía modificó la cláusula para aclarar que los derechos concedidos son únicamente los necesarios para el funcionamiento del navegador y no implican la propiedad sobre los datos del usuario. Ajit Varma, vicepresidente de Producto en Mozilla, aseguró que la intención nunca fue apropiarse de la información de los usuarios, sino mejorar la transparencia en el uso de los datos.

Para garantizar la privacidad, Mozilla enfatizó que no vende ni compra información personal y que los datos compartidos con socios son anonimizados y explicados en su aviso de privacidad. Se recomienda a los usuarios revisar periódicamente los términos de uso y la política de privacidad para conocer cómo se maneja su información, ajustar la configuración del navegador para reforzar su seguridad y mantenerse al tanto de las actualizaciones oficiales de Mozilla. También se sugiere utilizar extensiones de privacidad y herramientas de bloqueo de rastreadores para aumentar la protección de datos.

Prioridad: Importante

Ampliar Información:

https://thehackernews.com/2025/03/mozilla-updates-firefox-terms-again.html

---

Microsoft anuncia el cierre definitivo de Skype en mayo de 2025

Microsoft ha confirmado que cerrará Skype el 5 de mayo de 2025, poniendo fin a 22 años de servicio desde su lanzamiento en 2003. La decisión se enmarca en la estrategia de la compañía de centrar sus esfuerzos en Microsoft Teams, que ha experimentado un crecimiento significativo en los últimos años. Skype, que revolucionó las comunicaciones en línea con sus llamadas de voz y video, ha perdido relevancia debido a la competencia de otras plataformas como Zoom y WhatsApp. Para facilitar la transición, Microsoft permitirá a los usuarios iniciar sesión en Teams con sus credenciales actuales, migrando automáticamente sus contactos y chats. La compañía recomienda a los usuarios exportar cualquier dato importante antes de la fecha de cierre y explorar las funcionalidades de Teams para adaptarse al cambio.

El anuncio ha sido identificado por expertos en tecnología como una medida de optimización, ya que Microsoft busca consolidar sus servicios de comunicación en una única plataforma más moderna y versátil. Se aconseja a los usuarios migrar a Teams cuanto antes para familiarizarse con la interfaz y evitar inconvenientes cuando Skype deje de estar disponible. Además, es recomendable respaldar mensajes y archivos esenciales que puedan necesitar en el futuro, así como evaluar otras alternativas de comunicación en caso de que Teams no cubra sus necesidades. Microsoft asegura que esta transición permitirá una mejor integración con herramientas de productividad y mayor seguridad en las comunicaciones.

Prioridad: Importante.

Ampliar Información:

https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-its-killing-off-skype-in-may-after-14-years/