GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1825

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	1	0	0
MALWARE	0	1	0
NOTICIAS DE CIBERSEGURIDAD	0	0	2

VULNERABILIDADES

Alerta en Crestron Automate VX: vulnerabilidad de transmisión en texto claro (CVE-2025-47419) expone credenciales

Una vulnerabilidad crítica identificada como CVE-2025-47419 afecta a los dispositivos Crestron Automate VX, permitiendo la transmisión de información sensible, como contraseñas de usuario, en texto claro a través de la interfaz web y la API. Esta falla, clasificada como CWE-319: Transmisión de Información Sensible en Texto Claro, permite que un atacante intercepte y acceda a datos confidenciales mediante la captura del tráfico de red.

La vulnerabilidad impacta a las versiones de Automate VX desde la 5.6.8161.21536 hasta la 6.4.0.49. La empresa ha lanzado la actualización 6.4.1.8, que desactiva el acceso a través de puertos no seguros, mitigando así el riesgo.

Los CVE relacionados a este compromiso de seguridad son:

CVE-2025-47419

Recomendaciones de mitigación:

- Actualizar a la versión 6.4.1.8 o superior de Crestron Automate VX para asegurar la desactivación de puertos no seguros.
- Deshabilitar temporalmente el acceso a través de puertos no seguros si la actualización inmediata no es posible.
- Implementar monitoreo de red para detectar transmisiones no cifradas de información sensible.
- Revisar y fortalecer las políticas de seguridad relacionadas con la transmisión de datos en texto claro.

Prioridad: Crítico.

Ampliar Información:

- https://nvd.nist.gov/vuln/detail/CVE-2025-47419
- https://github.com/advisories/GHSA-49xp-c6gp-qwww
- https://secalerts.co/vulnerability/CVE-2025-47419
- https://www.crestron.com/security
- https://www.crestron.com/release_notes/automate_vx_6.4.1.8_release_notes.pdf

Recomendaciones generales sobre vulnerabilidades:

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

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Serve

2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Alerta: Módulos maliciosos de Go distribuyen malware que borra discos en sistemas Linux

Investigadores de ciberseguridad han identificado una campaña de ataque a la cadena de suministro que utiliza módulos maliciosos de Go para distribuir malware capaz de sobrescribir completamente el disco principal de sistemas Linux, dejándolos inoperables. Los módulos afectados contienen código ofuscado que descarga y ejecuta scripts destructivos.

Módulos maliciosos identificados:

- github.com/truthfulpharm/prototransform
- github.com/blankloggia/go-mcp
- github.com/steelpoor/tlsproxy

Estos módulos, al ejecutarse en sistemas Linux, descargan un script que sobrescribe el dispositivo /dev/sda con ceros, eliminando todos los datos y haciendo que el sistema no pueda arrancar.

Recomendaciones para mitigar el riesgo:

- Evitar el uso de módulos de fuentes no verificadas: Instalar únicamente paquetes de repositorios oficiales y mantenidos activamente.
- Revisar y auditar dependencias regularmente: Utilizar herramientas de análisis de dependencias para identificar posibles amenazas.
- Implementar controles de seguridad en el entorno de desarrollo: Restringir permisos y monitorear actividades sospechosas.
- Realizar copias de seguridad periódicas: Asegurar que los datos críticos puedan recuperarse en caso de incidentes.

Prioridad: Urgente.

Ampliar Información:

- https://thehackernews.com/2025/05/malicious-go-modules-deliver-disk.html
- https://securityaffairs.com/177411/malware/malicious-go-modules-designed-to-wipe-linux-systems.html
- https://www.bleepingcomputer.com/news/security/linux-wiper-malware-hidden-in-malicious-go-modules-on-github/
- https://securityaffairs.com/177411/malware/malicious-go-modules-designed-to-wipe-linux-systems.html
- https://www.linkedin.com/posts/randall-barnett-villalobos_malicious-go-modules-deliver-disk-wiping-activity-7324456997444083713-44hk
- https://securityaffairs.com/177411/malware/malicious-go-modules-designed-to-wipe-linux-systems.html
- https://gbhackers.com/hackers-weaponize-go-modules-to-deliver-disk%E2%80%91wiping-malware/

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

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

NOTICIAS DE CIBERSEGURIDAD

Alerta en comunicaciones gubernamentales: clon de Signal utilizado por funcionarios estadounidenses comprometido por ciberataque

Un reciente ciberataque comprometió TM Signal, una versión modificada de la aplicación de mensajería Signal, utilizada por funcionarios del gobierno de Estados Unidos, incluyendo al congresista Mike Waltz. La aplicación, desarrollada por la empresa israelí TeleMessage y posteriormente adquirida por la firma estadounidense Smarsh, fue diseñada para permitir el archivado de mensajes, sacrificando el cifrado de extremo a extremo que caracteriza a Signal original.

El ataque permitió a los ciberdelincuentes acceder a registros de chat sin cifrar, nombres de usuario, contraseñas y claves de cifrado, lo que representa una grave amenaza para la confidencialidad de comunicaciones gubernamentales. Tras conocerse la intrusión,

Smarsh suspendió el servicio de TM Signal e inició una investigación con el apoyo de una firma externa de ciberseguridad.

Adicionalmente, el senador Ron Wyden ha solicitado una investigación del Departamento de Justicia, resaltando que TM Signal no estaba aprobado por FedRAMP, lo que significa que no cumplía los estándares federales de seguridad para su uso oficial.

Recomendaciones para organizaciones:

1. Suspender el uso de aplicaciones no autorizadas para comunicaciones sensibles, especialmente en entornos gubernamentales o empresariales críticos.
2. Adoptar soluciones de mensajería con cifrado de extremo a extremo, sin funciones de archivado que comprometan la confidencialidad.
3. Educar al personal sobre las políticas de seguridad y los riesgos del uso de herramientas no aprobadas.
4. Auditar las aplicaciones utilizadas en entornos sensibles para asegurar que cumplen las normativas y estándares de seguridad requeridos.

Prioridad: Importante.

Ampliar Información:

- https://www.wired.com/story/tm-signal-telemessage-plaintext-message-archive/
- https://www.perplexity.ai/page/hackers-access-signal-clone-us-uy1lO.yjSCqM.XSkrJczqA
- https://www.theverge.com/news/661173/telemessage-signal-clone-hacked-mike-waltz
- https://www.404media.co/the-signal-clone-the-trump-admin-uses-was-hacked/

Análisis: aplicaciones de la inteligencia artificial en la operación de redes según LACNIC

El artículo de LACNIC titulado "¿Qué puede aportar la inteligencia artificial a la operación de redes?" explora cómo la inteligencia artificial (IA) y el aprendizaje automático (ML) están comenzando a integrarse en la gestión y operación de redes. Esta iniciativa responde a una demanda creciente de la comunidad técnica por comprender y aplicar estas tecnologías en entornos de red.

Puntos clave del artículo:

- Aplicación del aprendizaje automático en redes: Christian Rothenberg, investigador de la Universidad de Campinas, presenta cómo técnicas de ML, originalmente diseñadas para tareas como la predicción de precios o la clasificación de imágenes, están siendo adaptadas para optimizar operaciones de red. Esto incluye la detección de anomalías, la automatización de configuraciones y el análisis predictivo del tráfico.
- Inteligencia artificial generativa en la gestión de redes: Carlos Martínez, CTO de LACNIC, aborda el uso de IA generativa, destacando su potencial en la generación automática de configuraciones, análisis de eventos y documentación. Estas herramientas pueden mejorar la eficiencia y reducir errores humanos en la operación de redes.
- Demanda de la comunidad técnica: La iniciativa surge de una escucha activa a la comunidad, identificando una necesidad concreta de conocer más sobre la aplicación de IA y ML en redes

Recomendaciones para profesionales de redes:

- Explorar herramientas de ML: Investigar y probar soluciones de aprendizaje automático que puedan integrarse en la infraestructura de red existente.

- Capacitación en IA generativa: Formarse en el uso de herramientas de IA generativa para tareas como la generación de configuraciones y documentación automática.
- Participar en eventos y talleres: Asistir a sesiones como las ofrecidas por LACNIC para mantenerse actualizado sobre las últimas tendencias y aplicaciones de IA en redes.

Prioridad: Importante.

Ampliar Información:

https://blog.lacnic.net/que-puede-aportar-la-inteligencia-artificial-a-la-operacion-de-redes/