Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 077	Fecha: 30-03-2023
		Página 4 de 29

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Código fuente de Twitter se filtró en Github, revelando información patentada y fallas de seguridad		
Tipo de ataque	Filtración de datos	Abreviatura	FdD
Medios de propagación	Red, Internet		
Código de familia	K	Código de subfamilia	K01
Clasificación temática familia	Filtración y Exposición de Datos		

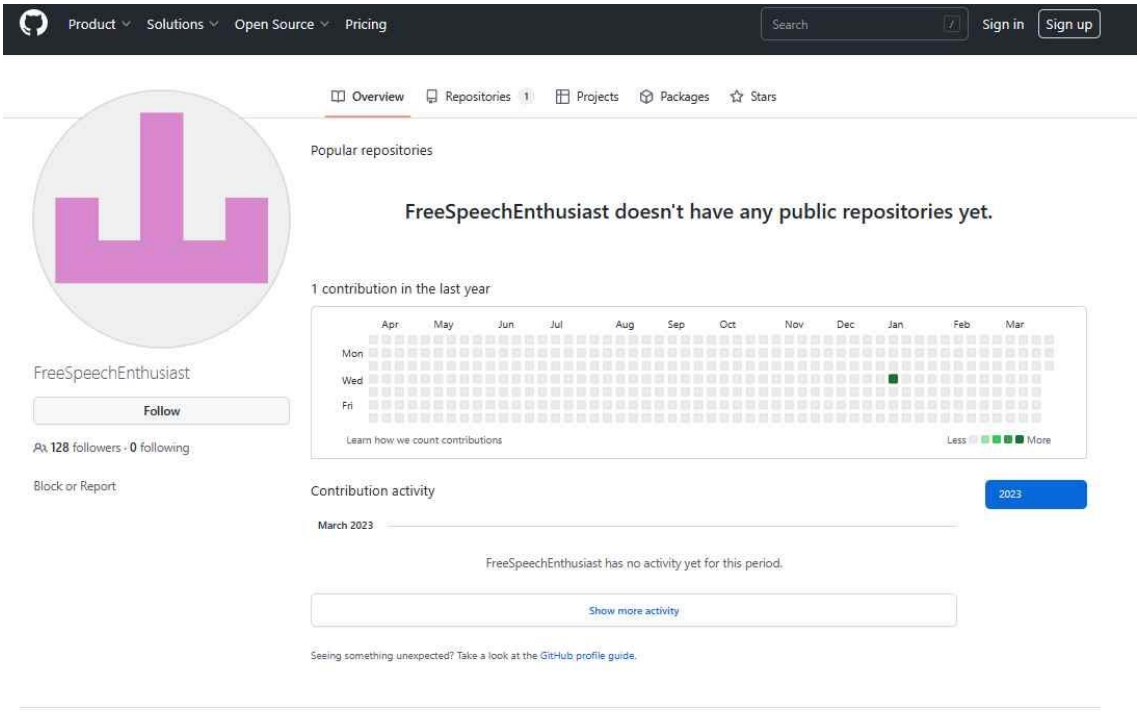
Descripción

Twitter sufrió una filtración significativa cuando partes significativas de su código fuente se publicaron en línea y se hicieron públicos.

La corporación procedió de inmediato a notificar a GitHub, sobre una violación de derechos de autor para eliminar el código robado del sitio. No se sabe cuánto tiempo estuvo disponible el código en línea, aunque parece haber sido accesible al público durante varios meses.

DETALLES:

- Twitter ha presentado una petición ante el Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California solicitando que el tribunal exija a GitHub que revele la identidad de la persona responsable de difundir el código, así como de cualquier otro usuario que lo haya descargado.



- Una de las principales preocupaciones de Twitter es que el código que fue robado tiene fallas de seguridad que podrían proporcionar a los ciberdelincuentes u otras partes con intenciones maliciosas las herramientas para acceder a los datos del usuario o tal vez dejar fuera de línea el sitio web por completo.

- Por otro lado, a Twitter le preocupa que la filtración pueda dar lugar a una filtración de datos o a un ciberataque, los cuales podrían ser muy perjudiciales para la imagen de la empresa y podrían provocar importantes pérdidas financieras.

- Actualmente Twitter tiene que abordar tanto el problema de la filtración como las posibles fallas de seguridad que se han puesto de manifiesto como resultado de la filtración.

RECOMENDACIONES:

- Utilizar métodos de autenticación robustos, es decir claves largas y complejas, difíciles de "adivinar" y que no contengan información del usuario que fácilmente se pueda inferir, como nombres de familiares, lugares y fechas personales y familiares, etc.
- Usar métodos de doble autenticación.
- No compartir las claves ni datos personales por medios no.

Fuentes de información	▪ hxxps://noticiasseguridad.com/hacking-incidentes/el-codigo-fuente-de-twitter-se-filtro-en-github-revelando-informacion-patentada-y-fallas-de-seguridad/ ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 077	**Fecha: 30-03-2023**
		Página 9 de 29

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	La falla del protocolo WiFi permite a los atacantes secuestrar el tráfico de la red		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

ANTECEDENTES:

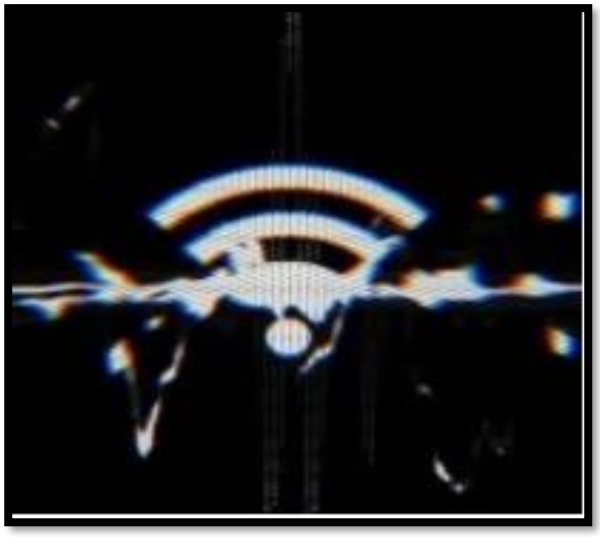
El 28 de marzo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha observado que Los investigadores de seguridad cibernética han descubierto una falla de seguridad fundamental en el diseño del estándar de protocolo WiFi IEEE 802.11, que permite a los atacantes engañar a los puntos de acceso para filtrar marcos de red en forma de texto sin formato.

Las tramas WiFi son contenedores de datos que constan de un encabezado, una carga útil de datos y un tráiler, que incluyen información como la dirección MAC de origen y destino, y los datos de control y administración.

Estas tramas se ordenan en colas y se transmiten de forma controlada para evitar colisiones y maximizar el rendimiento del intercambio de datos al monitorear los estados ocupado/inactivo de los puntos de recepción.

DETALLES:

Los investigadores descubrieron que las tramas en cola/en búfer no están adecuadamente protegidas de los adversarios, que pueden manipular la transmisión de datos, la suplantación de identidad del cliente, la redirección de tramas y la captura.



"Nuestros ataques tienen un impacto generalizado ya que afectan a varios dispositivos y sistemas operativos (Linux, FreeBSD, iOS y Android) y porque pueden ser utilizados para secuestrar conexiones TCP o interceptar tráfico web y de clientes", se lee en el documento técnico publicado ayer por Domien Schepers y Aanjhan Ranganathan de la Universidad Northeastern, y Mathy Vanhoef de imec-DistriNet, KU Leuven.

Este ataque es posible utilizando herramientas personalizadas creadas por los investigadores llamadas MacStealer, que pueden probar las redes WiFi para eludir el aislamiento del cliente e interceptar el tráfico destinado a otros clientes en la capa MAC.

Los investigadores advierten que estos ataques podrían usarse para inyectar contenido malicioso, como JavaScript, en paquetes TCP. "Un adversario puede usar su propio servidor conectado a Internet para inyectar datos en esta conexión TCP al inyectar paquetes TCP fuera de ruta con una dirección IP de remitente falsificada", advierten los investigadores.

"Esto puede, por ejemplo, abusarse para enviar código JavaScript malicioso a la víctima en conexiones HTTP de texto sin formato con el objetivo de explotar vulnerabilidades en el navegador del cliente". Si bien este ataque también podría usarse para espiar el tráfico, dado que la mayoría del tráfico web está encriptado mediante TLS, el impacto sería limitado.

El malware ladrón generalmente se propaga a través de diferentes canales, incluidos archivos adjuntos de correo electrónico, descargas de software falsas y otras técnicas de ingeniería social.

RECOMENDACIONES:

- Se recomienda aplicar medidas de mitigación como el uso de mecanismos de aplicación de políticas a través de un sistema como Cisco Identity Services Engine (ISE), que puede restringir el acceso a la red mediante la implementación de tecnologías Cisco TrustSec o Software Defined Access (SDA).

- Cisco también recomienda implementar la seguridad de la capa de transporte para cifrar los datos en tránsito siempre que sea posible, ya que el atacante inutilizaría los datos adquiridos", se lee en el aviso de seguridad de Cisco.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/wifi-protocol-flaw-allows-attackers-to-hijack-network-traffic/