Investigadores cibernéticos de Check Point revelaron este jueves los detalles de una vulnerabilidad menor, pero de fácil explotación en Zoom, el software de videoconferencia bastante popularizado en los últimos meses.

Esta última falla de Zoom podría haber permitido a los atacantes imitar a una organización, engañando a sus empleados o socios comerciales para que revelen información personal u otra información confidencial utilizando trucos de ingeniería social.

Aunque los ataques de ingeniería social pueden sonar no muy prácticos, un ataque similar fue utilizado este miércoles para hackear cuentas de Twitter de alto perfil como parte de una estafa de criptomonedas.

La vulnerabilidad reside en la función de URL personalizable de Zoom, denominada Vanity URL, con el objetivo de permitir a las empresas crear una URL personalizada en su subdominio y página de inicio de marca, como *«tuempresa.zoom.us»*, donde el enlace de invitación a una reunión se parece utilizando variantes de subdominio y dominio.

El equipo de investigadores de Check Point descubrió que debido a una validación incorrecta de la cuenta, cualquier ID de reunión podría haberse lanzado utilizando la URL de vanidad de cualquier organización, incluso si una reunión fue configurada por una cuenta individual separada.

> *«El problema de seguridad se centra en las funcionalidades del subdominio. Hay varias formas de ingresar a una reunión que contiene un subdominio, incluido el uso de un enlace directo de subdominio que contiene la ID de la reunión o el uso de la interfaz de usuario web personalizada del subdominio de la organización»*, dijeron los investigadores.

Los atacantes pueden explotar la vulnerabilidad de dos formas:

- Ataque a través de enlaces directos: Un hacker puede cambiar la URL de invitación,

incluyendo un subdominio registrado de su elección, al configurar una reunión. Un usuario que recibe el enlace de invitación, puede caer en la trampa del atacante, pensando que se trata de una invitación genuina por parte de una organización real.
- Atacar interfaces web dedicadas de Zoom: Debido a que algunas organizaciones tienen su interfaz web Zoom para llamadas de conferencia, un pirata informático también podría apuntar a dicha interfaz e intentar redirigir a un usuario para que ingrese una ID de reunión en la URL maliciosa en lugar de la interfaz web real de Zoom.

El impacto de este problema puede llevar a un intento de phishing exitoso, permitiendo a los atacantes hacerse pasar por un empleado legítimo de la compañía, lo que potencialmente les permite robar credenciales e información confidencial y llevar a cabo otras acciones de fraude.

Los investigadores de Check Point revelaron de forma responsable el problema a Zoom Video Communications Inc. y trabajaron juntos para abordarlo y establecer salvaguardas adicionales para la protección de los usuarios.

> *«Debido a que Zoom se ha convertido en uno de los principales canales de comunicación del mundo para empresas, gobiernos y consumidores, es crítico que se impida a los actores de amenazas explotar Zoom con fines criminales»,* dijo Adi Ian, Gerente de Grupo en Check Point Research.
>
> *«Trabajando junto con el equipo de seguridad de Zoom, hemos ayudado a Zoom a proporcionar a los usuarios de todo el mundo una experiencia de comunicación más segura, simple y confiable para que puedan aprovechar al máximo los beneficios del servicio»,* agregó.

A inicios del año, Check Point Research también trabajó con Zoom para parchear un error grave de privacidad que podría haber permitido que personas no invitadas se unan a

reuniones privadas y escuchen de forma remota audio, video y documentos privados compartidos durante la sesión.

Hace tan solo una semana, Zoom parchó una vulnerabilidad de día cero en todas las versiones compatibles del cliente Zoom para Windows, que podría haber permitido a un atacante ejecutar código arbitrario en computadoras con Windows 7 o anterior.