Microsoft informó que no corregirá tres de las cuatro vulnerabilidades de seguridad descubiertas en su plataforma de comunicación empresarial Teams a inicios de marzo.

La divulgación proviene de la firma de seguridad cibernética, Positive Security, con sede en Berlín, que descubrió que la implementación de la función de vista previa del enlace era susceptible a una serie de problemas que podrían *«permitir el acceso a los servicios internos de Microsoft, falsificar la vista previa del enlace y, para los usuarios de Android, filtrar su dirección IP y realizar DoS'in a sus aplicaciones/canales de Teams».*

De las cuatro vulnerabilidades, se dice que Microsoft ha abordado solo una que da como resultado la fuga de direcciones IP de los dispositivos Android, y la compañía dijo que se considerará una solución para la falla de denegación de servicio (DoS) en una versión futura del producto. Los problemas fueron comunicados responsablemente a la empresa el 10 de marzo de 2021.

La principal de las fallas es una vulnerabilidad de falsificación de solicitudes del lado del servidor (SSRF) en el punto final *«/urlp/v1/url/info»* que podría explotarse para obtener información de la red local de Microsoft.

También se descubre un error de suplantación de identidad en el que el objetivo del enlace de vista previa se puede modificar para que apunte a cualquier URL maliciosa mientras se mantiene intacto el enlace principal, la imagen de vista previa y la descripción, lo que permite a los atacantes ocultar enlaces maliciosos y realizar ataques de phishing mejorados.

La vulnerabilidad DoS, que afecta a la versión de Android de Teams, podría hacer que la aplicación se bloquee simplemente enviando un mensaje con una vista previa de enlace especialmente diseñada que contiene un objetivo no válido en lugar de una URL legítima.

El último de los problemas se refiere a una fuga de direcciones IP, que también afecta a la aplicación de Android. Al interceptar mensajes que incluyen una vista previa del enlace para apuntar la URL en miniatura a un dominio que no es de Microsoft, Positive Security dijo que es posible obtener acceso a la dirección IP de un usuario y a los datos del agente del usuario.

> *«Aunque las vulnerabilidades descubiertas tienen un impacto limitado, es sorprendente tanto que aparentemente no se hayan probado vectores de ataques tan simples como antes, y que Microsoft no tenga la voluntad o los recursos para proteger a sus usuarios de ellas»,* dijo el cofundador de Positive Security, Fabian Bräunlein.