Microsoft lanzó la semana pasada actualizaciones para el navegador Edge con correcciones para dos problemas de seguridad. Uno de estos se refiere a una vulnerabilidad de omisión de seguridad que podría explotarse para inyectar y ejecutar código arbitrario en el contexto de cualquier sitio web.

Rastreada como CVE-2021-34506, con puntaje CVSS de 5.4, la debilidad se debe a un problema de scripting universal entre sitios (UXSS), que se activa cuando se traducen de forma automática páginas web utilizando la función incorporada del navegador a través de Microsoft Translator.

Ignacio Laurence, Vansg Devgan y Shivam Kumar Singh fueron acreditados con CyberXplore Private Limited por descubrir y reportar CVE-2021-34506.

> *«A diferencia de los ataques XSS comunes, UXSS es un tipo de ataque que explota las vulnerabilidades del lado del cliente en las extensiones del navegador con el fin de generar una condición de XSS, y ejecutar código malicioso»,* dijeron los investigadores de CyberXplore.
>
> *«Cuando se detectan y explotan estas vulnerabilidades, el comportamiento del navegador se ve afectado y sus funciones de seguridad pueden omitirse o desactivarse»,* agregaron.

Específicamente, los investigadores encontraron que la función de traducción contenía un fragmento de código vulnerable que no pudo desinfectar la entrada, lo que permitió al atacante insertar potencialmente código JavaScript malicioso en cualquier lugar de la página web que luego se ejecuta cuando el usuario hace clic en el mensaje en la barra de direcciones para traducir la página.

Como exploit de prueba de concepto (PoC), los investigadores demostraron que era posible desencadenar el ataque con el simple hecho de agregar un comentario a un video de

YouTube, que está escrito en un idioma diferente al inglés, junto con una carga útil XSS.

De forma similar, se descubrió que una solicitud de amistad de un perfil de Facebook que tenía contenido en otro idioma y la carga útil XSS ejecutaba el código tan pronto como el destinatario de la solicitud verificaba el perfil del usuario.

Después de la divulgación responsable el 3 de junio, Microsoft solucionó el problema el 24 de junio, además de otorgar a los investigadores 20 mil dólares como parte de su programa de recompensas por errores.

La última versión 91.0.864.59 del navegador web basado en Chromium se puede descargar el Configuración y más > Acerca de Microsoft Edge, o en edge://settings/help.