Investigadores de ciberseguridad descubrieron una falla crítica en la popular extensión de Evernote para Chrome, que podría haber permitido a los hackers secuestrar el navegador y robar información confidencial de cualquier sitio web al que se haya accedido.

Evernote es un popular servicio que ayuda a las personas a crear notas y organizar sus listas de tareas pendientes, su extensión para Chrome ha sido utilizada por más de 4,610,000 usuarios.

Descubierta por Guardio, la vulnerabilidad identificada como CVE-2019-12592, residía en las formas en que la extensión de Evernote Web Clipper interactúa con los sitios web, iframes y scripts de inyección, y finalmente, rompiendo la política del mismo origen (SOP) y los mecanismos de aislamiento del dominio.

Según los investigadores, la vulnerabilidad podría permitir que un sitio web controlado por un atacante ejecute código arbitrario en el navegador en el contexto de otros dominios en nombre de los usuarios, lo que llevaría a un problema de secuencias de comandos entre sitios universales (UXSS o Universal XSS).

> *«Un exploit completo que permitiría cargar un script controlado por un pirata informático remoto en el contexto de otros sitios web se puede lograr por medio de un solo comando simple winow.postMessage. Al abusar de la infraestructura de inyección prevista de Evernote, el script malicioso se inyectará en todos los marcos de destino en la página, independientemente de las restricciones de origen cruzado»,* dijeron los investigadores.

Como se observa en el video, los investigadores también desarrollaron un exploit de prueba de concepto (PoC) que puede inyectar una carga útil personalizada en sitios web específicos y robar cookies, credenciales y otra información privada de un usuario desprevenido.

Ya que las extensiones se ejecutan en el navegador web, generalmente requieren la capacidad de realizar solicitudes de red, acceder y cambiar el contenido de las páginas que

se visitan, lo que representa una amenaza masiva para la privacidad y seguridad, sin importar si ha sido instalada desde tiendas oficiales de Firefox o Chrome.

> *«Aunque el autor de la aplicación pretende brindar una mejor experiencia de usuario, las extensiones generalmente tienen permisos para acceder a una gran cantidad de recursos sensibles y representan un riesgo de seguridad mucho mayor que los sitios web tradicionales»*, agregaron los investigadores.

El equipo de Guardio informó sobre el problema a Evernote a finales del mes pasado, la compañía luego lanzó una versión actualizada y parcheada de su extensión Evernote Web Clipper para usuarios de Chrome.

Generalmente Chrome buscar versiones de las extensiones instaladas para actualizar cada 5 horas, por lo que debes asegurarte de que tu navegador ejecute la última versión de Evernote 7.11.1 o posterior.