Una vulnerabilidad de seguridad recientemente corregida en el navegador web Microsoft Edge pudo haber sido explotada para instalar extensiones arbitrarias en los sistemas de los usuarios y llevar a cabo acciones maliciosas.

> Según un nuevo informe compartido por el investigador de seguridad de Guardio Labs, Oleg Zaytsev, *«Esta vulnerabilidad habría permitido a un atacante utilizar una API privada, originalmente destinada a fines de marketing, para instalar extensiones adicionales en el navegador de manera encubierta y sin el conocimiento del usuario».*

La vulnerabilidad, conocida como CVE-2024-21388 (con una puntuación CVSS de 6.5), fue abordada por Microsoft en la versión estable 121.0.2277.83 de Edge, lanzada el 25 de enero de 2024, después de que se reportara responsablemente en noviembre de 2023. Tanto Zaytsev como Jun Kokatsu fueron acreditados por informar sobre el problema.

«Un atacante que explotara con éxito esta vulnerabilidad podría obtener los privilegios necesarios para instalar una extensión», señaló Microsoft en un aviso sobre la falla, agregando que *«podría resultar en una fuga del sandbox del navegador».*

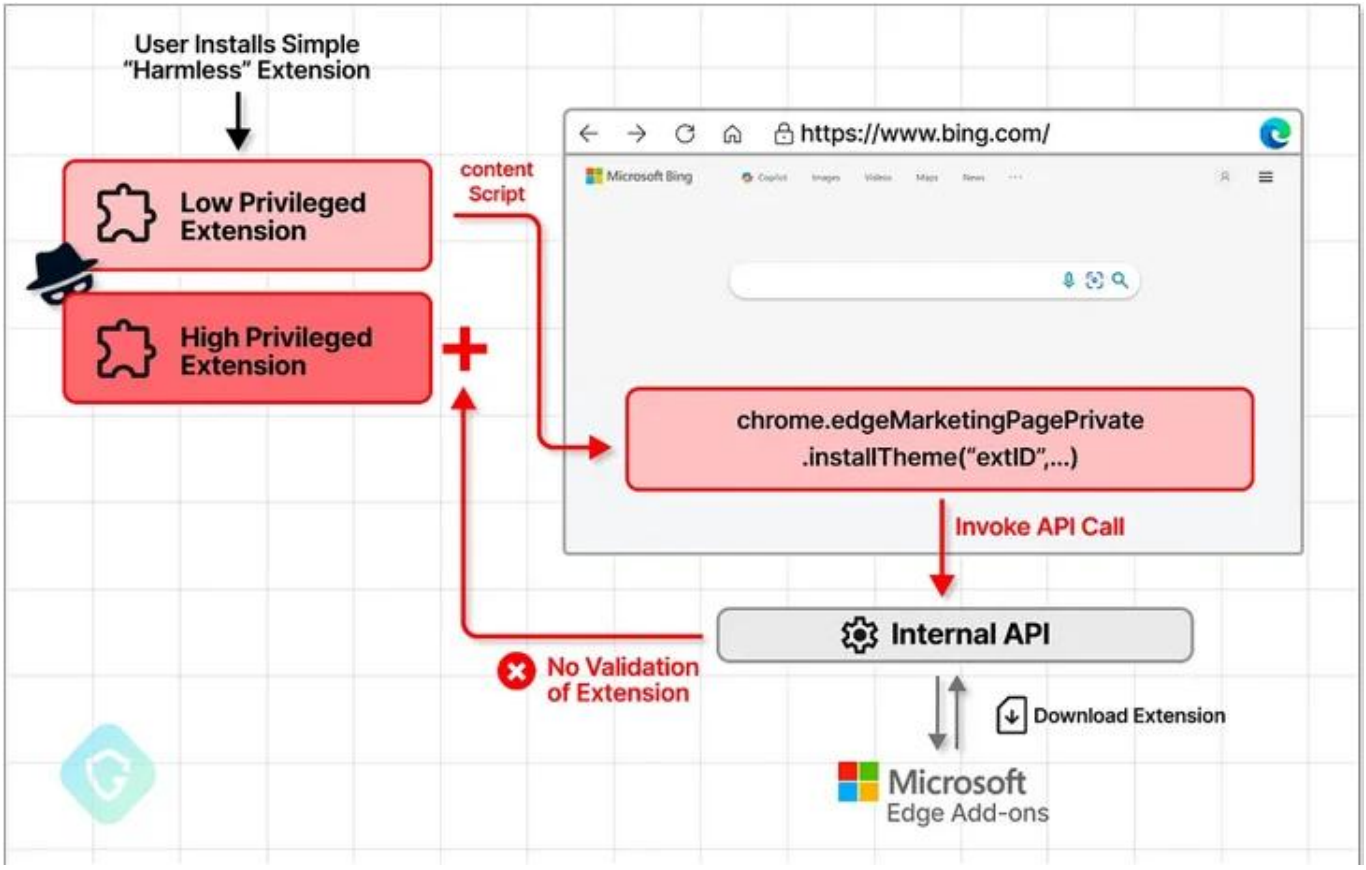
Según la descripción de Microsoft, se trata de una falla de escalada de privilegios que requiere que un atacante realice acciones adicionales antes de la explotación para preparar el entorno objetivo.

De acuerdo con los hallazgos de Guardio, la vulnerabilidad CVE-2024-21388 permitiría a un atacante con capacidad para ejecutar JavaScript en las páginas de bing[.]com o microsoft[.]com instalar cualquier extensión desde la tienda de complementos de Edge sin requerir el consentimiento del usuario.

Esto se debe a que el navegador tiene acceso privilegiado a ciertas API privadas que permiten la instalación de extensiones siempre y cuando provengan de la propia tienda de extensiones del proveedor.

Una de estas API, llamada edgeMarketingPagePrivate, es accesible desde una lista de sitios web permitidos que pertenecen a Microsoft, incluyendo bing[.]com, microsoft[.]com, microsoftedgewelcome.microsoft[.]com y microsoftedgetips.microsoft[.]com, entre otros.

La API también incluye un método llamado installTheme() que, como su nombre indica, está diseñado para instalar un tema desde la tienda de complementos de Edge al proporcionar un identificador único de tema («themeId») y su archivo de manifiesto como entrada.



El error identificado por Guardio es esencialmente un caso de validación insuficiente, lo que permite a un atacante proporcionar cualquier identificador de extensión de la tienda (en lugar del themeId) y hacer que se instale sigilosamente.

> *«Como ventaja adicional, dado que esta instalación de la extensión no se realiza de la manera originalmente diseñada, no será necesario ningún tipo de interacción o consentimiento por parte del usuario»*, explicó Zaytsev.

En un escenario hipotético de ataque aprovechando CVE-2024-21388, un actor malicioso podría publicar una extensión aparentemente inofensiva en la tienda de complementos y usarla para inyectar un fragmento de código JavaScript malicioso en bing[.]com, o en cualquiera de los sitios que tengan acceso a la API, y luego instalar una extensión arbitraria de su elección invocando la API utilizando el identificador de extensión.

En otras palabras, ejecutar la extensión especialmente creada en el navegador Edge y dirigirse a bing[.]com instalará automáticamente la extensión objetivo sin el permiso de la víctima.

Guardio informó que aunque no hay evidencia de que este error haya sido explotado en la naturaleza, destaca la necesidad de equilibrar la comodidad del usuario y la seguridad, y cómo las personalizaciones del navegador pueden inadvertidamente desactivar los mecanismos de seguridad e introducir varios nuevos vectores de ataque.

> *«Es relativamente fácil para los atacantes engañar a los usuarios para que instalen una extensión que parece inofensiva, sin darse cuenta de que sirve como el primer paso en un ataque más complejo. Esta vulnerabilidad podría ser explotada para facilitar la instalación de extensiones adicionales, potencialmente con fines de lucro»*, dijo Zaytsev.