El miércoles, Google lanzó actualizaciones para solucionar cuatro vulnerabilidades de seguridad en su navegador web Chrome, entre ellas una que, según la compañía, ya está siendo aprovechada activamente.

Esta falla crítica, identificada como CVE-2025-4664 (con una puntuación CVSS de 4.3), está relacionada con una aplicación inadecuada de políticas de seguridad dentro de un componente denominado *Loader*.

Según la descripción del problema:

> *«Una aplicación insuficiente de políticas en Loader en Google Chrome antes de la versión 136.0.7103.113 permitía que un atacante remoto filtrara datos entre orígenes mediante una página HTML especialmente diseñada.»*

Google atribuyó el hallazgo al investigador en seguridad Vsevolod Kokorin (@slonser_), quien compartió los detalles de la vulnerabilidad en X el 5 de mayo de 2025. La empresa también reconoció que «existe un exploit para CVE-2025-4664 que circula activamente».

Kokorin explicó en una serie de publicaciones:

> *«A diferencia de otros navegadores, Chrome resuelve la cabecera Link en solicitudes de subrecursos. El problema es que dicha cabecera puede definir una referrer-policy. Podemos establecer unsafe-url y capturar los parámetros completos de la consulta.»*

Además, señaló que dichos parámetros pueden contener información sensible, lo que podría facilitar la toma de control total de una cuenta. Esta información, agregó, puede ser robada mediante la carga de una imagen alojada en un recurso de terceros.

Aunque no se ha confirmado si esta vulnerabilidad ha sido utilizada en ataques reales más allá de la demostración de prueba de concepto (PoC), CVE-2025-4664 se convierte en la segunda falla en ser explotada activamente, después de CVE-2025-2783.

Como medida preventiva, se recomienda a los usuarios actualizar Chrome a las versiones 136.0.7103.113 o 136.0.7103.114 en Windows y Mac, y a la versión 136.0.7103.113 en Linux. También se aconseja a los usuarios de navegadores basados en Chromium —como Microsoft Edge, Brave, Opera y Vivaldi— aplicar las actualizaciones correspondientes en cuanto estén disponibles.