Google parcheó una vulnerabilidad de día cero en el navegador web Chrome para escritorio, que actualmente está siendo explotada en la naturaleza.

La compañía lanzó la versión 88.0.4324.150 para Windows, Mac y Linux, con una solución para una falla de desbordamiento de búfer de pila (CVE-2021-21148) en su motor de renderizado V8 JavaScript.

> *«Google está al tanto de los informes de que existe un exploit para CVE-2021-21158 en la naturaleza»*, dijo la compañía en un comunicado.

El investigador Mattias Buelens fue quien informó a Google sobre la falla de seguridad el 24 de enero de 2021.

El 2 de febrero, Google abordó seis vulnerabilidades, entre ellas, una vulnerabilidad en Pagos (CVE-2021-21142) y cuatro fallas de alta gravedad en las funciones de Extensiones, Grupos de pestañas, Fuentes y Navegación.

Aunque es típico de Google limitar los detalles de vulnerabilidades hasta que la mayoría de los usuarios estén actualizados con la solución, el desarrollo se produce semanas después de que Google y Microsoft revelaran los ataques llevados a cabo por hackers norcoreanos contra investigadores de seguridad con una elaborada campaña de ingeniería social para instalar una backdoor de Windows.

Con algunos investigadores infectados por el simple hecho de visitar un blog de investigación falso en sistemas completamente parcheados que ejecutan Windows 10 y el navegador Chrome, Microsoft informó el 28 de enero, que había insinuado que los atacantes probablemente aprovecharon un 0-day de Chrome para comprometer los sistemas.

Aunque no está claro si CVE-2021-21148 se utilizó en dichos ataques, el momento de las revelaciones y el hecho de que el aviso de Google salió exactamente un día después de que Buelens informara el problema, implica que podrían estar relacionados.

En un artículo separado, la compañía de seguridad cibernética de Corea del Sur, ENKI, dijo que el grupo de hackers patrocinado por el estado norcoreano conocido como Lazarus, intentó fallidamente atacar a sus investigadores de seguridad con archivos HTML maliciosos que, al abrirse, descargaron dos cargas útiles de un servidor remoto, de los cuales, uno contenía un día cero contra Internet Explorer.

> *«La carga útil secundaria contiene el código de ataque contra la vulnerabilidad del navegador Internet Explorer»,* dijeron los investigadores de ENKI.

Cabe mencionar que el año pasado, Google arregló cinco vulnerabilidades de día cero que fueron explotadas activamente en la naturaleza en un lapso de un mes entre el 20 de octubre y el 12 de noviembre.