Nro. Alerta:	AL-2024-011	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	30-may-2024	**Vulnerabilidad CVE-2024-5274 en Google Chrome**	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistemas y/o software Abierto

Nivel de riesgo: Alto

II. ALERTA

Google Chromium V8 contiene una vulnerabilidad de confusión de tipos que permite a un atacante remoto ejecutar código a través de una página HTML diseñada. Esta vulnerabilidad con el código CVE-2024-5274, podría afectar a varios navegadores web que utilizan Chromium, incluidos, entre otros, Google Chrome, Microsoft Edge y Opera.

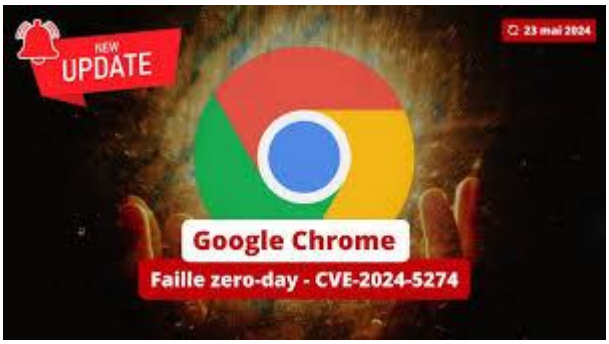

Figura 1: *CVE-2024-5274, figura referencial*
Fuente: https://www.it-connect.fr/cve-2024-5274-la-8eme-faille-zero-day-de-2024-corrigee-dans-google-chrome/

III. INTRODUCCIÓN

El motor V8, desarrollado por Google, es una pieza fundamental en el ecosistema del navegador Google Chrome. Su principal tarea es interpretar y ejecutar el código JavaScript presente en las páginas web de manera eficiente y rápida

De código abierto y escrito en C++, también es utilizado por Node.js (entorno en tiempo de ejecución multiplataforma de JavaScript por el lado del servidor), entre otras aplicaciones. Si bien los otros navegadores más populares tienen su propio motor de

JavaScript (Firefox tiene SpiderMonkey y Safari JavaScriptCore) Microsoft Edge y Opera utilizan actualmente el motor V8.

La velocidad y eficiencia del motor V8 en Google Chrome se deben a su enfoque en la compilación y ejecución de código JavaScript. V8 en Google Chrome utiliza una técnica innovadora llamada compilación en tiempo real, que convierte el código JavaScript en código de máquina altamente optimizado. Esto permite que las aplicaciones web se ejecuten más rápido y respondan de manera más veloz a las interacciones del usuario. V8 corre en Mac, Windows, Linux y su nombre es una suerte de homenaje al diseño y potencia de los motores V8 de los automóviles, donde la disposición de los 8 cilindros forma una V.

Un problema de seguridad fue descubierto internamente por un investigador de Google y se lo identificó con el código CVE-2024-5274. Se trata de una 'confusión de tipos' de alta gravedad en V8, por lo que Google ha lanzado con urgencia otra actualización para abordar esta octava vulnerabilidad de día cero en el navegador Chrome.

Una vulnerabilidad de "confusión de tipos" ocurre cuando un programa asigna una porción de memoria para contener un cierto tipo de datos pero interpreta erróneamente los datos como un tipo diferente. Esto puede provocar fallos, corrupción de datos y ejecución de código arbitrario.

Google no ha compartido detalles técnicos sobre la falla; sin embargo, la solución de Google se está implementando en el canal estable de Chrome en la versión 125.0.6422.112/.113 para Windows y Mac, mientras que los usuarios de Linux recibirán la actualización en la versión 125.0.6422.112 en las próximas semanas.

IV. VECTOR DE ATAQUE:

CVE-2024-5274: Vulnerabilidad clasificada como crítica. Esta vulnerabilidad afecta a una parte desconocida del componente V8. La manipulación con una entrada desconocida conduce a una vulnerabilidad de confusión de tipos. La definición CWE para la vulnerabilidad es CWE-843. El producto asigna o inicializa un recurso como un puntero, objeto o variable usando un tipo, pero luego accede

a ese recurso usando un tipo que es incompatible con el tipo original. Se sabe que este impacto afecta la confidencialidad, la integridad y la disponibilidad.

El ataque se puede iniciar de forma remota. No se requiere ningún tipo de autenticación para una explotación exitosa; se requiere la interacción del usuario por parte de la víctima. Se desconocen los detalles técnicos, pero hay un exploit público disponible.

V. RECOMENDACIONES:

- Aplicar las actualizaciones emitidas por los fabricantes.

VI. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VII. REFERENCIAS:

- https://keepcoding.io/blog/v8-en-google-chrome/
- https://fusiona.cl/blog/tecnologia/v8-el-motor-javascript-tras-google-chrome/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://vuldb.com/?id.266122
- https://www.bleepingcomputer.com/news/security/google-fixes-eighth-actively-exploited-chrome-zero-day-this-year/
- https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_23.html