I. DATOS GENERALES:

Clase de alerta: Vulnerabilidades

Tipo de incidente: Vulnerabilidades

Nivel de riesgo: Alto

II. ALERTA

Se han detectado múltiples vulnerabilidades en el navegador Google Chrome, y que de ser explotadas, los ciber atacantes podrían ejecutar código malicioso comprometiendo los sistemas y activos de información, a través de la instalación no autorizada de aplicaciones, modificación y borrado de archivos, y creación de cuentas de usuarios con perfiles administrativos.

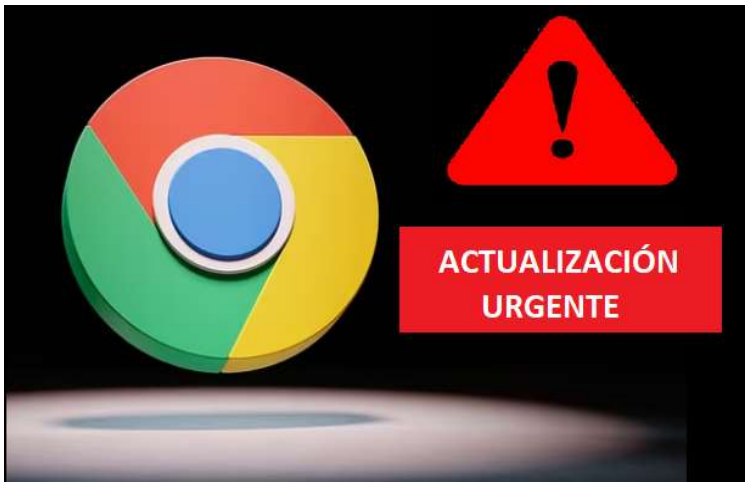

Figura 1.- lustración relacionada a vulnerabilidades Google Chrome
Fuente: Elaboración Propia

III. INTRODUCCIÓN

Investigadores han detectado múltiples vulnerabilidades en Google Chrome, dentro de las cuales se encuentran posibilidades de ejecución de código malicioso. Los detalles técnicos de las vulnerabilidades y la explotación de las mismas están categorizadas como tácticas de Acceso Inicial y técnicas de comprometimiento de sistemas.

Las vulnerabilidades detectadas en Google Chrome hacen uso de todas las características del perfil de usuario en el que se explotaron las vulnerabilidades, por lo tanto en primera instancia el alcance del comprometimiento del sistema es proporcional al perfil de usuario.

Las versiones vulnerables de Chrome son las versiones anteriores a la 116.0.5845 para Windows y 116.0.5845 para Mac y Linux, y el riesgo de manera general para organizaciones ha sido estimado como alto. Las características técnicas específicas de la explotación de las vulnerabilidades detectadas en Google Chrome, se encuentran registradas en los formularios de priorización de riesgos cve, según el siguiente detalle:

- CVE-2023-4761
- CVE-2023-4762
- CVE-2023-4763
- CVE-2023-4764

IV. VECTOR DE ATAQUE:

- Uso de la aplicación Google Chrome en dispositivos.

V. IMPACTO:

- Instalación no autorizada de aplicaciones.

- Modificación y borrado de archivos
- Creación de cuentas de usuario con perfiles administrativos.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar la aplicación a las versiones más recientes de acuerdo al desarrollador.
- Aplicar el principio de menor privilegio respecto de la creación de perfiles de usuario.
- Restringir la interacción con sitios web respecto de actividades de descarga y ejecución de archivos.
- Informar a usuarios respecto de amenazas provenientes en enlaces remitidos a través de correos electrónicos..

VII. REFERENCIAS:

Yip, D. Google Chrome. Stable Channel Update for Desktop. (5 de 09 de 2023). Obtenido de https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop.html.

- NIST. CVE-2023-4761. (04 de 09 de 2023). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4761
- NIST. CVE-2023-4762. (04 de 09 de 2023). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4762
- NIST. CVE-2023-4763. (04 de 09 de 2023). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4763
- NIST. CVE-2023-4764. (04 de 09 de 2023). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4764