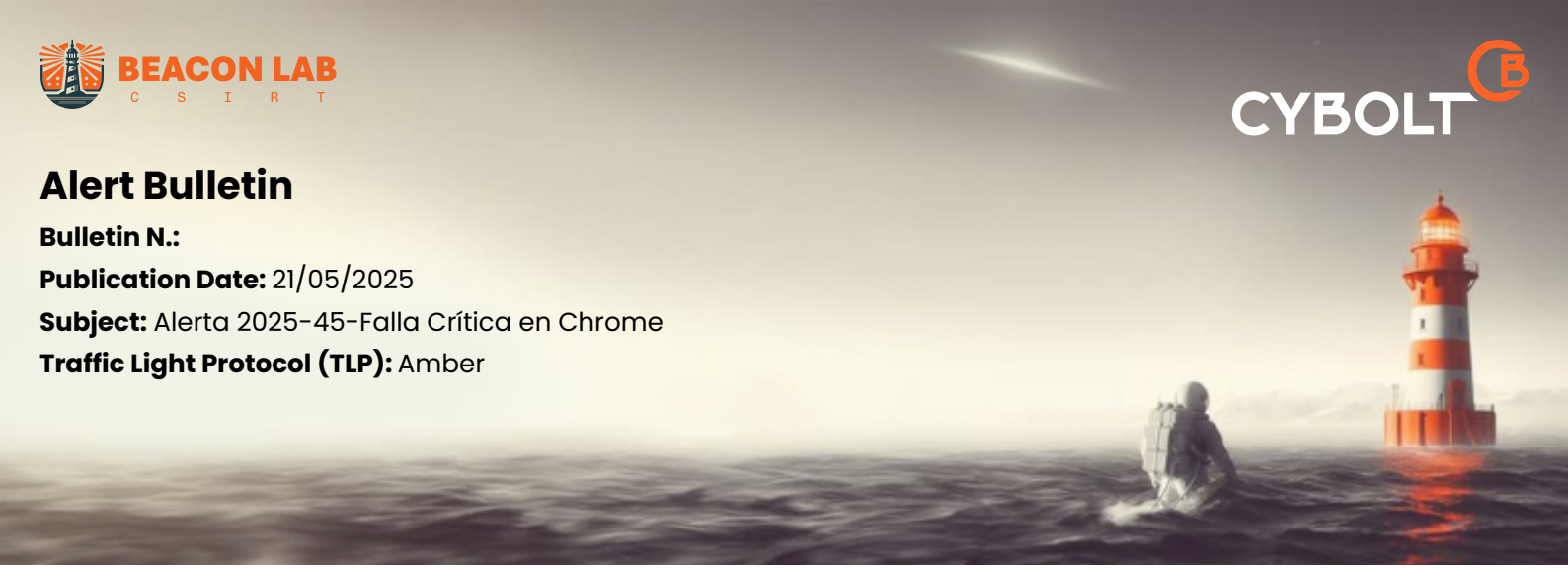

Alert Bulletin

Bulletin N.:
Publication Date: 21/05/2025
Subject: Alerta 2025-45-Falla Crítica en Chrome
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Google Chrome anterior a la versión 136.0.7103.113

Descripción

Se ha identificado una **vulnerabilidad en Google Chrome**, registrada como **CVE-2025-4664**, que afecta al componente **Chrome Loader**, encargado de gestionar la carga de imágenes, scripts y otros recursos dentro de los sitios web.

El fallo se origina porque **Chrome no aplicaba correctamente las políticas de seguridad entre sitios web** (conocidas como "***Same-Origin Policy***"). Esta debilidad permitía que un atacante accediera a **URLs completas**, incluyendo **información sensible** como **tokens de sesión, claves de autenticación** o **identificadores personales**.

Bastaba con **visitar un sitio web malicioso**, sin necesidad de descargar archivos o hacer clic, para que el atacante pudiera insertar **recursos ocultos** (como imágenes) que provocaran la **fuga de datos confidenciales** sin que el usuario lo percibiera.
Nivel de riesgo: Bajo (CVSS 4.3)

Solución:

Actualizar Chrome inmediatamente a la versión:

- 136.0.7103.113/.114 en Windows y Mac
- 136.0.7103.113 en Linux

Las actualizaciones las puede encontrar aquí

- https://support.google.com/chrome/answer/95346?hl=es&co=GENIE.Platform%3DDesktop

Mitigaciones adicionales:

- **Evite visitar sitios web de procedencia dudosa**, no haga clic en enlaces sospechosos ni descargue contenido de fuentes no verificadas. Esta vulnerabilidad puede ser explotada simplemente al visitar una página web maliciosa, sin necesidad de interacción adicional.
- Incluso sitios legítimos pueden ser comprometidos mediante ataques del tipo watering hole, por lo que se recomienda mantener una navegación prudente, especialmente en entornos corporativos o donde se maneje información sensible.
- **Para administradores de sistemas y sitios web**:
- Monitoree continuamente la integridad de sus servidores web y aplicaciones para detectar signos de compromiso.
- Implemente herramientas de detección de amenazas y revise periódicamente los archivos alojados en su sitio.
- Refuerce las configuraciones de seguridad y asegúrese de que todo el software del servidor esté actualizado.

Información adicional:

- https://www.malwarebytes.com/blog/news/2025/05/update-your-chrome-to-fix-serious-actively-exploited-vulnerability?utm_campaign=brandsocial&utm_medium=social&utm_source=twitter
- https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-4664
- https://thehackernews.com/2025/05/new-chrome-vulnerability-enables-cross.html