



BOLETÍN DE ALERTA

Boletín Nro.: 2022-46

Fecha de publicación: 28/10/2022

Tema: Vulnerabilidad de día cero (*0-day*) en Google Chrome

Las versiones afectadas son:

- Google Chrome, versiones anteriores a 107.0.5304.87 (para Windows, Mac y Linux)

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad de día cero (*0-day*) que afecta a Google Chrome, que permitiría a un atacante acceder a información confidencial y provocar ejecución de código arbitrario. La vulnerabilidad está siendo explotada activamente.

La vulnerabilidad identificada como [CVE-2022-3723](#), de severidad “alta”, sin una puntuación asignada aún. Esta vulnerabilidad de día cero (*0-day*) se debe a una falla dentro del componente *V8 JavaScript* de Google Chrome. Dicha falla denominada *Type confusion* sucede cuando un programa asigna o inicializa un recurso como un puntero, objeto o variable usando un tipo (*type*) específico, pero luego accede a ese recurso usando otro tipo (*type*) que es incompatible con el original, causando el acceso a memoria fuera de los límites.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante acceder a información confidencial y provocar ejecución de código arbitrario.

Solución:

Recomendamos realizar la actualización de Google Chrome correspondiente a la versión 107.0.5304.87/.88 (para Windows) o 107.0.5304.87 (para Mac y Linux) a través del siguiente enlace:

- <https://www.google.com/chrome/>

Información adicional:

- <https://securityonline.info/cve-2022-3723-google-chrome-0-day-vulnerability/>
- https://chromereleases.googleblog.com/2022/10/stable-channel-update-for-desktop_27.html
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3723>
- <https://www.google.com/chrome/>

Ciberseguridad y Protección de la Información

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Gral. Santos y Concordia - Complejo Santos - Offic. E14

cert@cert.gov.py | +595 21 217 9000

Asunción - Paraguay | www.cert.gov.py

