BOLETIN INFORMATIVO

TLP: CLEAR

Vulnerabilidad Crítica en Google Chrome (CVE-2025-2783)

Se identificó una grave vulnerabilidad de día cero en el navegador Google Chrome, clasificada como **CVE-2025-2783**, la cual permite a los atacantes evadir el entorno seguro del navegador (sandbox) y ejecutar código malicioso en el equipo. También afecta a otros navegadores basados en Chromium como Edge, Brave, Opera y Vivaldi. Esta vulnerabilidad ha sido detectada en la versión 134.0.6998.177/.178 de Chrome para Windows.

Esta falla ha sido explotada activamente en una campaña de ciberespionaje llamada ForumTroll, especialmente dirigida a periodistas, universidades y entidades gubernamentales. Los atacantes distribuyen archivos o enlaces maliciosos que instalan el malware StilachiRAT, una herramienta que roba credenciales, cookies, claves de criptomonedas y más.

Impacto:

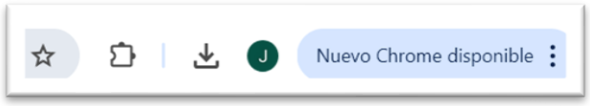
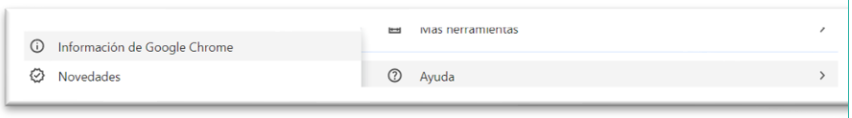
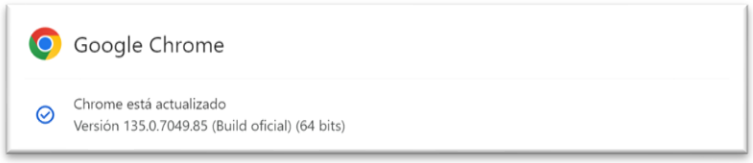
Vector 3.x: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Puntuación base 3.x: 8.30

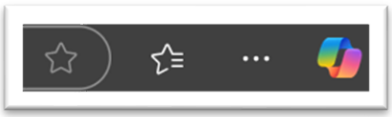
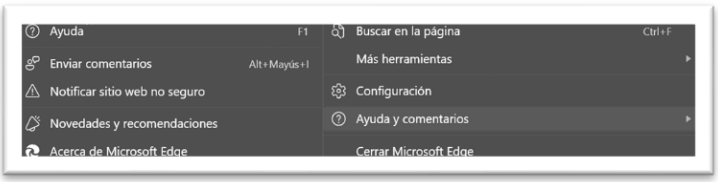
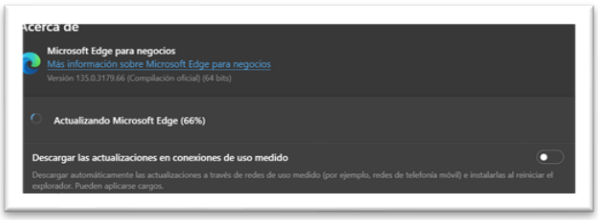
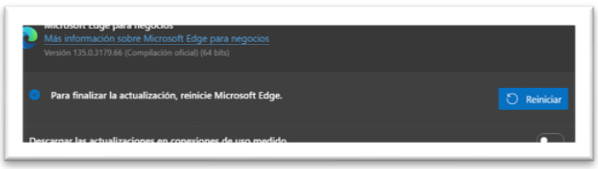
Gravedad: **ALTA**

Actividades de mitigacion:

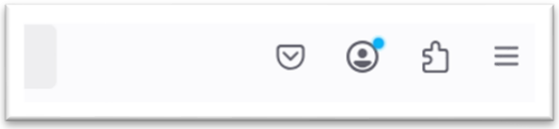
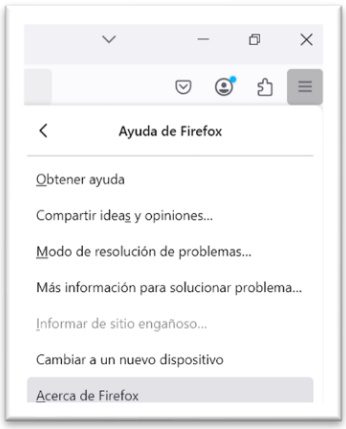
Actualizar el navegador Chrome manualmente a la versión 134.0.6998.88/.89 o superior.

Acción	Ilustración
Abrir Chrome	
Hacer clic en los tres puntos en la esquina superior derecha	
Seleccionar Ayuda > Información de Google Chrome	
Si hay una actualización disponible, haz clic en Buscar actualizaciones (Check for updates)	
Verificar que se cuenta con la última versión disponible	

Actualizar el navegador Microsoft Edge a la versión más reciente.

Acción	Ilustración
Abrir Microsoft Edge	
Hacer clic en los tres puntos en la esquina superior derecha	
Seleccionar Ayuda y comentarios > Acerca de Microsoft Edge	
Si hay una actualización el navegador realizará la búsqueda y dar click en Reiniciar para aplicar los cambios	 
Verificar que se cuenta con la última versión disponible	

Actualizar el navegador Firefox a la versión más reciente.

Acción	Ilustración
Abrir Microsoft Edge	
Hacer clic en los tres lineas en la esquina superior derecha	
Seleccionar Ayuda > Acerca de Firefox	
Si hay una actualización el navegador realizará la búsqueda y dar click en Reiniciar para aplicar los cambios	

Acción	Ilustración
	
Verificar que se cuenta con la última versión disponible	

En caso de utilizar navegadores diferentes a los mencionados anteriormente, tener en cuenta que se deben realizar las actividades de actualización según corresponda, con el fin de prevenir la explotación de la vulnerabilidad.

Recomendaciones:

- Forzar la actualización en los equipos corporativos y monitorear actividad inusual.
- Debido a que una de las maneras de ejecutar el ataque es mediante un correo phishing el cual incluye una invitación al foro internacional de ciencias económicas y políticas Primakov Readings, es necesario evitar abrir este tipo de correos o enlaces sospechosos provenientes de fuentes desconocidas.
- Verificar que se está usando una versión actualizada accediendo a: chrome://settings/help.
- Brindar capacitación a los usuarios finales frente al manejo que se debe brindar ante la sospecha del recibo de correos electrónicos maliciosos.

Fuentes:

Portal The Hacker NEWS:

https://thehackernews.com/2025/03/zero-day-alert-google-releases-chrome.html

Portal de soporte de Google:
https://support.google.com/chrome/answer/95414?hl=es-419&co=GENIE.Platform%3DDesktop

Portal de Kaspersky:
https://www.kaspersky.com/blog/forum-troll-apt-with-zero-day-vulnerability/53215/

CSIRT Salud
Dirección: Calle 119 No. 13 - 51, Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570
www.csirtsalud.gov.co