BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-51
Fecha de publicación: 10/10/2024
Tema: Vulnerabilidad Zero-Day Activamente Explotada en Firefox
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Firefox: versiones anteriores a 131.0.2
- Firefox ESR: versiones anteriores a 115.16.1 y 128.3.1

Descripción

Mozilla ha lanzado una actualización urgente para Firefox (versión 131.0.2) y Firefox ESR (versiones 115.16.1 y 128.3.1) para corregir una vulnerabilidad crítica de ejecución de código remoto, CVE-2024-9680. El popular navegador web de código abierto junto con su versión para empresas y organizaciones presentan un problema de *use-after-free* en las animaciones de la línea de tiempo, y ha sido activamente explotado en ataques. Un atacante puede aprovechar este error para ejecutar código malicioso en el proceso de contenido del navegador.

Es crucial actualizar a las últimas versiones para mitigar este riesgo. Las actualizaciones automáticas están habilitadas por defecto, pero quienes las tengan desactivadas deben verificar manualmente en "Configuración > General > Actualizaciones de Firefox". Además, el navegador Tor, que se basa en Firefox ESR, también ha sido actualizado para corregir este problema.

Solución

Mozilla ha lanzado actualizaciones para mitigar esta vulnerabilidad en las versiones afectadas por lo que se recomienda a todos los usuarios actualizar sus navegadores lo antes posible para evitar posibles explotaciones de esta vulnerabilidad.

Puedes encontrar más información y detalles en el sitio oficial de Mozilla.

Información adicional:

- https://www.helpnetsecurity.com/2024/10/10/cve-2024-9680/
- https://www.securityweek.com/firefox-131-update-patches-exploited-zero-day-vulnerability/
- https://thehackernews.com/2024/10/mozilla-warns-of-active-exploitation-in.html

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com