Boletín de alerta

Boletín Nro.: 33
Fecha de publicación: 01/04/2026
Tema: Alerta 2026-33 Vulnerabilidad Importante en Python
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Afecta versiones a Python 3.6+

Descripción

Se ha reportado una vulnerabilidad importante de tipo Inyección de Comando en el modulo webbrowser de Python, fue etiquetado como CVE-2026-4519 con score 7.0.

La API webbrowser.open() aceptaba guiones iniciales («–«) en las URLs, que ciertos navegadores interpretaban como opciones de línea de comandos, permitiendo ejecución arbitraria de comandos.

Un atacante podría manipular URLs maliciosas (ej. –version https://evil.com) para ejecutar comandos del sistema vía el navegador lanzado, como abrir shells o ejecutar scripts. Riesgo principal en apps desktop/GUI que abren enlaces dinámicos sin sanitizar input de usuarios.

Solución:

- **Actualiza Python** a versiones parcheadas (3.13+ o parches específicos).
- **Sanitiza URLs**: Rechaza guiones leading antes de pasar a webbrowser.open().
- **Alternativas seguras**: Usa subprocess con validación estricta o librerías como webbrowser-open parcheadas.

Información adicional:

- https://www.cve.org/CVERecord?id=CVE-2026-4519
- https://www.openwall.com/lists/oss-security/2026/03/20/1