Boletín de alerta

Boletín Nro.: 82
Fecha de publicación: 09/10/2025
Tema: Alerta 2025-82 Vulnerabilidad RCE en CrowdStrike Falcon
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- CrowdStrike Falcon Sensor anteriores a 7.28.20008

Descripción

CrowdStrike ha publicado un aviso de seguridad titulado «Problemas que afectan al sensor Falcon de CrowdStrike para Windows». En él se indican correcciones para dos problemas que afectan al sensor Falcon para Windows.

- **CVE-2025-42701**: Una condición de carrera de tiempo de verificación y tiempo de uso (TOCTOU) en Falcon Sensor para Windows podría permitir que un atacante que haya ejecutado código previamente en un host elimine archivos arbitrarios; Puntuación CVSS 3.1: 5.6 (Media).
- **CVE-2025-42706**: Existe un error lógico en Falcon Sensor para Windows que podría permitir que un atacante que haya ejecutado código previamente en un host elimine archivos arbitrarios. Puntuación CVSS 3.1: 6.5 (Media)

No hay indicios de que estas vulnerabilidades se estén explotando en la práctica. El equipo de detección y análisis de amenazas de CrowdStrike está monitoreando activamente si estos problemas se están explotando.

Solución:

Las correcciones para ambos problemas se incluyen en la última versión 7.29 del sensor Falcon para Windows. En las revisiones de las versiones 7.24 a 7.28 y en la revisión 7.16 para hosts con Windows 7/2008 R2. La revisión de la versión 7.24 también es una actualización para el sensor de Visibilidad a Largo Plazo (LTV) actual para Windows IoT.

Es importante actualizar a las versiones antes mencionadas. Dependiendo de la configuración de la solución, dicha actualización puede ser automática o debe realizarse de forma manual, es importante revisar este punto.

Información adicional:

- https://vuldb.com/es/?id.327643
- https://vuldb.com/?id.327642
- https://cyberpress.org/crowdstrike-falcon-bug/
- https://radar.offseq.com/threat/cve-2025-42706-cwe-346-origin-validation-error-in–c1ed59e3
- https://nvd.nist.gov/vuln/detail/CVE-2025-42706
- https://cybersecuritynews.com/crowdstrike-falcon-windows-sensor-vulnerability/