Boletín de alerta

Boletín Nro.: 95
Fecha de publicación: 03/09/2026
Tema: Alerta 2026-95 0-Day de Escalación de Privilegios mediante Abuso de Remediación de Macros de MS Office en Crowdstrike Falcon
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

CrowdStrike Falcon Sensor — Plataforma de seguridad endpoint (EDR)

Producto	Configuración vulnerable	Sistema operativo
CrowdStrike Falcon Sensor	Phase 3 — Optimal Protection con «Microsoft Office file malicious macro removal» habilitado	Windows 11 25H2 (totalmente actualizado)
CrowdStrike Falcon Sensor	Phase 3 — Optimal Protection con «Microsoft Office file malicious macro removal» habilitado	Windows Server 2025 (totalmente actualizado)

Descripción

Se ha reportado una posible vulnerabilidad 0-day de **escalación local de privilegios (LPE)** que afecta al **CrowdStrike Falcon Sensor** y se publicó el código fuente y binario compilado del exploit, que ha sido bautizado como **FalconFlank,.** Aún no hay un comunicado oficial por parte de Crowstrike.

La falla abusa del mecanismo de remediación de **macros maliciosas en archivos Microsoft Office** — una funcionalidad que opera con privilegios elevados dentro del sensor — para elevar los privilegios de un usuario local sin privilegios hasta el nivel **SYSTEM** en sistemas Windows completamente actualizados.

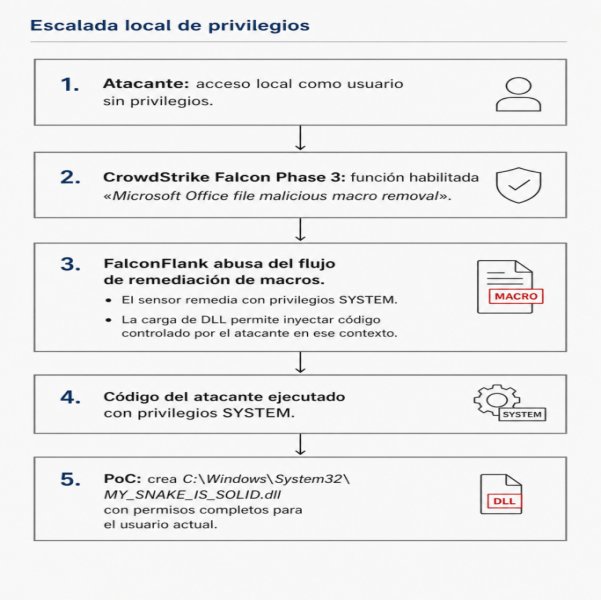

Figura 1 Flujo de explotación de FalconFlank

El investigador afirmó que la prueba de concepto funcionó en entornos **Windows 11 25H2 y Windows Server 2025** completamente actualizados y protegidos por CrowdStrike Falcon con la protección óptima de fase 3 habilitada.

El repositorio público se creó recientemente e incluye código fuente en C, una solución de Visual Studio, archivos de proyecto, archivos de cabecera y un directorio de lanzamiento compilado para x64.

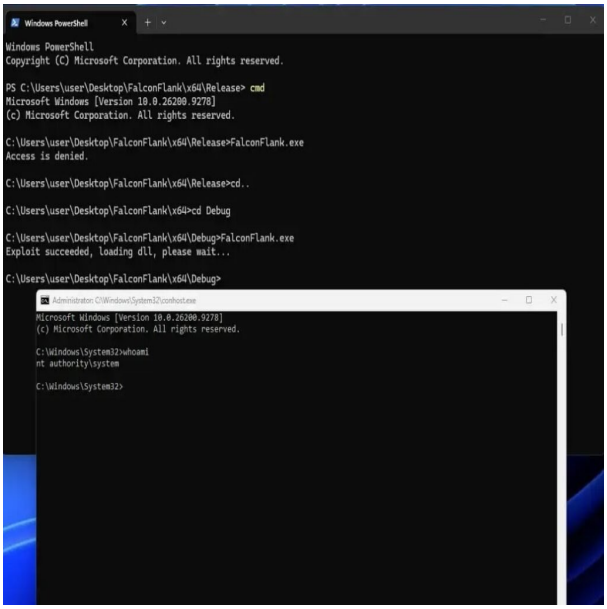

Figura 2 – Evidencia del PoC publicada por el investigador.

CrowdStrike ya ha emitido un comunicado informando que está investigando el asunto y que recomienda deshabilitar la funcionalidad temporalmente. Al hacerlo, las macros maliciosas ya no serán reemplazadas automáticamente, pero la protección continuará funcionando normalmente mediante Cloud Anti-malware for Microsoft Office Files, siempre que las políticas estén configuradas según las mejores prácticas.

Además, el exploit ya es detectado por Crowdstrike, sin embargo, es posible que un atacante sea capaz de evadir esa detección, por lo que es fundamental realizar la mitigación hasta tanto se cuente con un parche para la vulnerabilidad.

Mitigación

Mientras CrowdStrike emite un parche oficial:

- **Deshabilitar la opción "Microsoft Office File Suspicious Macro Removal"** dentro de la política de prevención de Windows, ubicada en *Next-gen antivirus > Clean infected Microsoft Office files*.
- **Monitorear la creación de archivos DLL en directorios del sistema** (C:\Windows\System32\) desde procesos del Falcon Sensor o procesos hijo inesperados.
    - Monitorearespecialmente cualquier alerta de detección del exploit FalconFlank
- **Monitorear el repositorio de CrowdStrike** (https://supportportal.crowdstrike.com) para la emisión de un advisory oficial o actualización del sensor.
- Tener en cuenta que el atacante **debe tener acceso local previo** — reforzar los controles de acceso, autenticación multifactor y políticas de least privilege en todos los endpoints protegidos con Falcon.

En el caso de clientes de Servicios administrados de Cybolt, el equipo del SOC ya ha aplicado las mitigaciones por lo que no es necesaria ninguna acción adicional en este momento.

Información adicional:

- **Para seguimiento:**
    - CrowdStrike Support Portal: https://supportportal.crowdstrike.com
    - CrowdStrike Security Advisories: https://www.crowdstrike.com/blog/category/security-advisories/
- https://cybersecuritynews.com/crowdstrike-falcon-0-day/