

Alert Bulletin

Bulletin N.: 95

Publication Date: 03/09/2026

Subject: Alert 2026-95 0-Day Privilege Escalation via Abuse of MS Office Macros Remediation in CrowdStrike Falcon

Traffic Light Protocol (TLP): White

Affected product(s):

CrowdStrike Falcon Sensor — Endpoint security platform (EDR)

Product	Vulnerable configuration	Operating system
CrowdStrike Falcon Sensor	Phase 3 — Optimal Protection with “Microsoft Office file malicious macro removal” enabled	Windows 11 25H2 (fully updated)
CrowdStrike Falcon Sensor	Phase 3 — Optimal Protection with “Microsoft Office file malicious macro removal” enabled	Windows Server 2025 (fully updated)

Description

A possible 0-day **local privilege escalation (LPE)** vulnerability affecting the **CrowdStrike Falcon Sensor** has been reported, and the source code and compiled binary of the exploit — dubbed **FalconFlank** — have been published. There is still no official statement from CrowdStrike.

The flaw abuses the remediation mechanism of **malicious macros in Microsoft Office files** — a feature that operates with elevated privileges within the sensor — to escalate the privileges of an unprivileged local user to **SYSTEM** level on fully updated Windows systems.

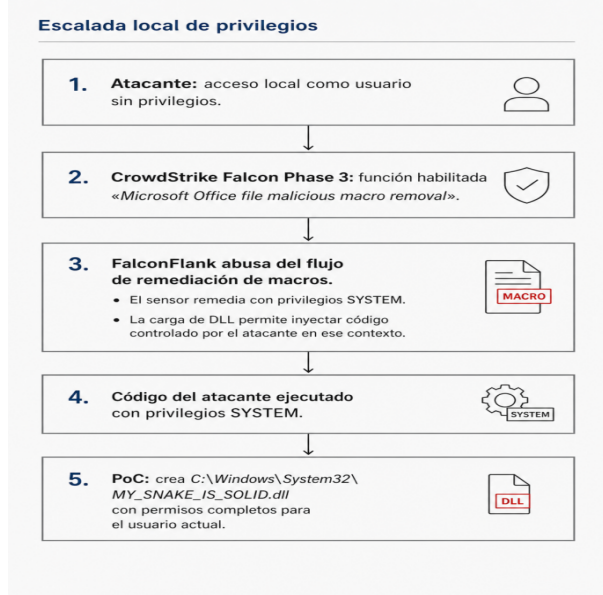


Figure 1 FalconFlank exploitation flow

The researcher stated that the proof of concept worked in fully updated [Windows 11 25H2](#) and [Windows Server 2025](#) environments protected by CrowdStrike Falcon with Phase 3 optimal protection enabled.

The public repository was recently created and includes C source code, a Visual Studio solution, project files, header files, and a release directory compiled for x64.

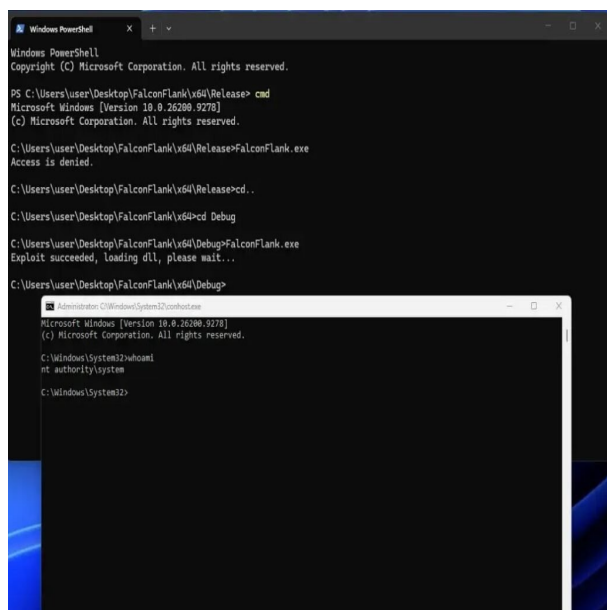


Figure 2 – Evidence of the PoC published by the researcher.

CrowdStrike has already issued a statement reporting that it is investigating the matter and recommends temporarily disabling the feature. When doing so, malicious macros will no longer be replaced automatically, but protection will continue to function normally through Cloud Anti-malware for Microsoft Office Files, provided that policies are configured according to best practices.

Additionally, the exploit is already detected by Crowdstrike; however, an attacker may be able to evade that detection, so it is essential to apply mitigation until a patch for the vulnerability is available.

Mitigation

While CrowdStrike issues an official patch:

- **Disable the option “Microsoft Office File Suspicious Macro Removal”** within the Windows prevention policy, located at *Next-gen antivirus > Clean infected Microsoft Office files*.
- **Monitor the creation of DLL files in system directories** (C:\Windows\System32\) from Falcon Sensor processes or unexpected child processes.
 - Especially monitor any detection alert for the FalconFlank exploit
- **Monitor the CrowdStrike repository** (<https://supportportal.crowdstrike.com>) for the issuance of an official advisory or sensor update.
- Keep in mind that the attacker **must have prior local access** — reinforce access controls, multi-factor authentication, and least privilege policies on all endpoints protected with Falcon.

For Cybolt Managed Services customers, the SOC team has already applied the mitigations, so no additional action is required at this time.

Additional information:

- **For follow-up:**
 - 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/>