BLACKSWAN CYBERSECURITY

THREAT ADVISORY
CrowdStrike Falcon Sensor Local Privilege Escalation Zero-Day (FalconFlank)

August 26, 2026

Severity: High
Status: Public Proof-of-Concept Released

Executive Summary

Security researcher Chaotic Eclipse (also known as MSNightmare, INFINITE NIGHTMARE, and Nightmare-Eclipse) has publicly released a proof-of-concept (PoC) exploit named **FalconFlank**, which claims to achieve **local privilege escalation (LPE) to NT AUTHORITY\SYSTEM** by abusing CrowdStrike Falcon Sensor's remediation process for malicious Microsoft Office macros. According to the researcher's public statements and GitHub repository, the exploit reportedly functions against **fully patched Windows 11 25H2 and Windows Server 2025 systems** running **CrowdStrike Falcon with "Microsoft Office file malicious macro removal" enabled**.

As of 2-Sept-26, CrowdStrike has not publicly confirmed the vulnerability, issued a CVE, released a security advisory, or provided remediation guidance. Independent validation of the claim has not been publicly reported. Multiple security news outlets have highlighted that the exploit remains an **unverified claim by the researcher** pending vendor analysis.

Despite the lack of vendor confirmation, the public availability of source code and a compiled PoC significantly increases the probability of additional researcher analysis, adversary testing, and attempted weaponization.

Threat Overview

FalconFlank specifically targets Falcon's remediation workflow associated with malicious Office macros. The researcher claims the security product's elevated remediation operations can be manipulated to create or load attacker-controlled content with SYSTEM-level permissions.

Technical Details

Based on the public GitHub README and subsequent reporting:

- FalconFlank allegedly abuses the Falcon Sensor's automated response capability for malicious Office macro remediation.
- The exploit reportedly allows a local user to leverage privileged remediation actions to gain SYSTEM access.
- The author states the PoC may already trigger CrowdStrike detections and suggests the DLL-loading mechanism could require modification to evade detection during testing.
- The exploit was reportedly tested against fully updated Windows builds protected by Falcon Phase 3 Optimal Protection.

THREAT ADVISORY
CrowdStrike Falcon Sensor Local Privilege Escalation Zero-Day (FalconFlank)

August 26, 2026

The exact root cause has not been publicly validated. Available reporting indicates the issue may involve unsafe handling of files or DLLs during Falcon's remediation workflow, but neither CrowdStrike nor an independent researcher has confirmed those details.

Potential Impact

If validated, exploitation could provide:

- Escalation from standard user privileges to SYSTEM.
- Bypass of endpoint security trust boundaries.
- Ability to disable or tamper with security tools.
- Credential theft opportunities.
- Persistence via privileged file modification.
- Enhanced ransomware deployment capabilities.
- Defense evasion against EDR controls.

Because Falcon operates with extensive operating system privileges, any weakness in its remediation pipeline could become a trusted path to privilege escalation.

MITRE ATT&CK Mapping

Tactic	Technique	Description
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1562.001	Impair Defenses
Execution	T1059	Command and Script Interpreter
Persistence	T1547	Boot/Logon Autostart Execution (possible post-exploitation)
Credential Access	T1003	OS Credential Dumping (potential follow-on activity)

TTP Analysis

Initial Access

FalconFlank is **not an initial access vector**.

An attacker must already have:

- Local interactive access
- Malware execution
- Remote access obtained through another attack chain

Privilege Escalation

Claimed Abuse of Falcon Remediation

The public PoC claims to:

1. Trigger Falcon's malicious Office macro remediation workflow.
2. Manipulate the remediation process.

3. Gain control over content processed by a SYSTEM-level security component.
4. Achieve SYSTEM privileges.

These details are currently based solely on researcher claims.

Defense Evasion
The PoC author explicitly notes that:
CrowdStrike may already detect the published exploit.

The author suggests:

- Using Falcon exclusions.
- Obfuscating the PoC.
- Modifying the DLL-loading mechanism.

These are statements made by the researcher and should not be interpreted as confirmed bypass methods.

Indicators of Compromise (IOCs)

High-Confidence IOC
The only concrete artifact publicly disclosed in reporting is:

IOC Type	Value
File Path	C:\Windows\System32\MY_SNAKE_IS_SOLID.dll

Security reporting cites the researcher as stating that successful execution may create this file with permissions that allow control by the current user.

Behavioral Indicators
Organizations should monitor for:

- Unexpected DLL creation or modification within:
  - C:\Windows\System32\
- Falcon remediation events immediately preceding privilege-escalation activity.
- Unusual SYSTEM-level child processes triggered shortly after Office-file remediation.
- Changes to Falcon exclusions.
- Suspicious Office document remediation actions involving user-writable content.

These are defensive hunting recommendations based on the reported attack class and are not confirmed IOCs.

THREAT ADVISORY
CrowdStrike Falcon Sensor Local Privilege Escalation Zero-Day (FalconFlank)

August 26, 2026

Detection Opportunities

EDR/SIEM Queries

Monitor for:

- New DLLs written to protected system directories.
- SYSTEM processes spawning from Falcon-related services.
- Privilege-escalation events immediately after Falcon remediation events.
- Sysmon Event ID 11 (File Create) in protected directories.
- Windows Event 4688 indicating unexpected SYSTEM-level process creation.

Recommended Actions

Immediate

1. Validate whether "Microsoft Office file malicious macro removal" is enabled within Falcon policies.
2. Review endpoints for unexpected DLL creation in:
    - C:\Windows\System32
3. Increase monitoring of Falcon remediation events.
4. Track CrowdStrike advisories and sensor updates closely.
5. Restrict local administrator rights wherever possible.
6. Alert SOC personnel regarding published FalconFlank PoC activity.

Short Term

- Conduct threat hunting focused on:
    - Privilege-escalation events
    - DLL loads from unusual locations
    - Falcon exclusion modifications
- Evaluate application control policies (AppLocker/WDAC).
- Inventory endpoints protected by Falcon Phase 3 policies.

Strategic

Because a public exploit now exists, organizations should assume:

- Reverse engineering efforts are occurring.
- Reliability improvements to the PoC will likely emerge.
- Threat actors will test the technique in lab environments.
- Vendor guidance could change rapidly as validation progresses.

Assessment

THREAT ADVISORY
CrowdStrike Falcon Sensor Local Privilege Escalation Zero-Day (FalconFlank)

August 26, 2026

Current Confidence: Medium-Low

Reason: Public PoC and source code exist, but vendor confirmation, CVE assignment, independent validation, and evidence of exploitation in the wild have not been reported.

Business Risk: High if validated, due to the potential for escalation directly through a trusted security agent running with elevated privileges.