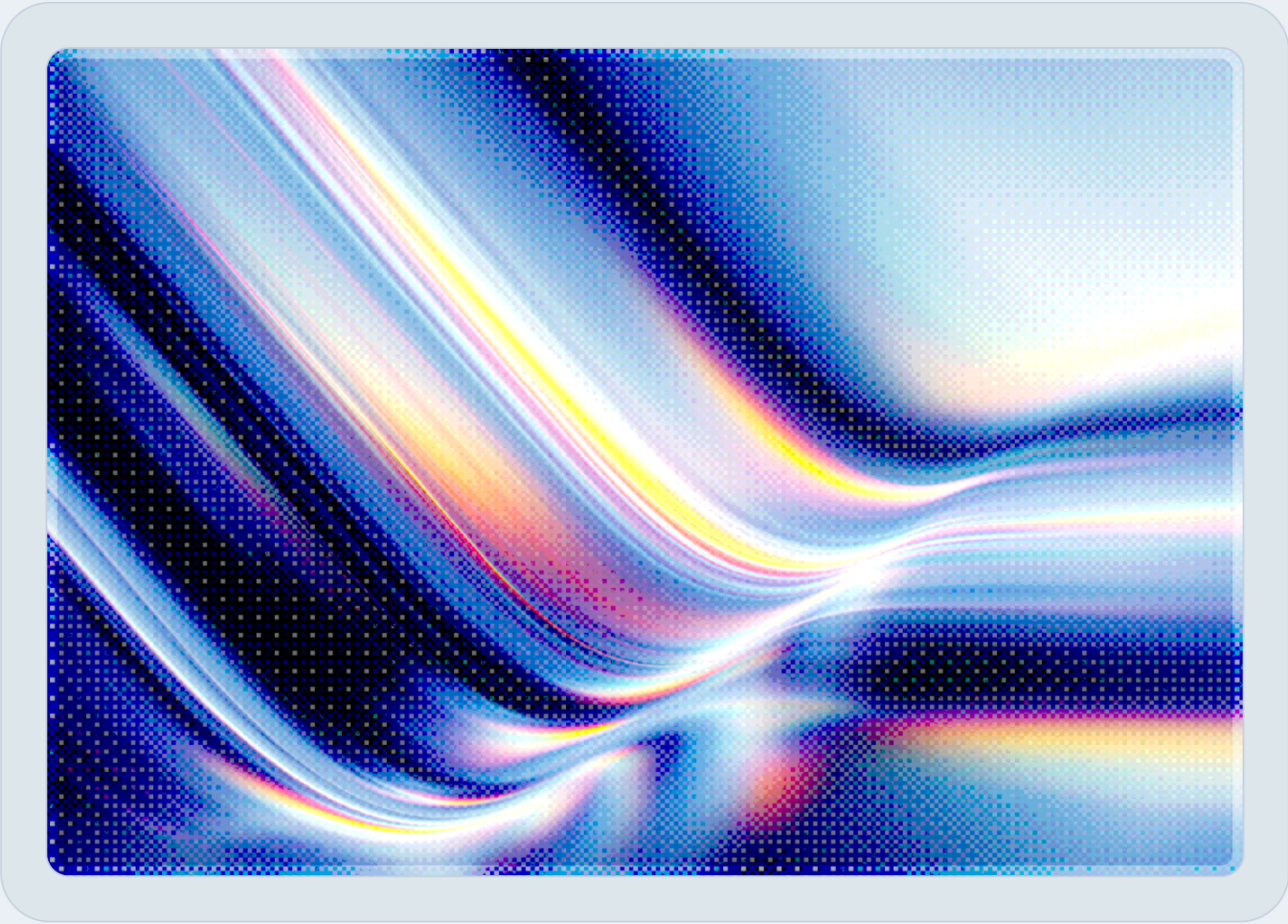
CSAI Foundation | Cloud Security Alliance

FalconFlank: CrowdStrike Falcon Zero-Day Grants SYSTEM Access

2026-09-06

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

"FalconFlank" is an unpatched, publicly disclosed privilege escalation vulnerability in CrowdStrike Falcon Sensor that lets a low-privileged local user obtain NT AUTHORITY\SYSTEM access on fully updated Windows 11 (25H2) and Windows Server 2025 endpoints [1][2].

A working proof-of-concept was published to GitHub on September 3, 2026, without prior coordination with CrowdStrike; no CVE identifier or CVSS score has been assigned, and no vendor patch is available as of this writing [1][3].

The exploit abuses Falcon's "Microsoft Office File Suspicious Macro Removal" remediation feature — a capability that necessarily runs with elevated privileges to clean malicious macros from Office documents — turning the sensor's own defensive logic against itself [1][6].

The researcher behind the disclosure, who publishes under the aliases Chaotic Eclipse, Nightmare Eclipse, MSNightmare, and INFINITE NIGHTMARE, has a documented history of releasing uncoordinated exploits against Kaspersky and Microsoft Defender before turning to CrowdStrike [5]. Combined with the Microsoft Defender disclosure discussed below, this pattern is consistent with a deliberate, cross-vendor campaign against endpoint security vendors generally, and — for the cases where the mechanism has been documented — against privileged remediation pipelines specifically.

CrowdStrike has acknowledged the report and is "actively investigating," and in the interim recommends disabling the Microsoft Office File Suspicious Macro Removal policy setting; organizations that do so remain protected through Falcon's separate Cloud Anti-malware for Microsoft Office Files capability [1][5].

Because the attack requires the affected remediation feature to be enabled and a specific Falcon prevention posture ("Phase 3 — Optimal Protection") to be configured, organizations should audit their own Falcon policy configuration immediately rather than assume the exposure is uniform across their fleet [3].

Background

CrowdStrike Falcon is a widely deployed endpoint detection and response (EDR) platform in the enterprise market, and its sensor runs with kernel-level and system-level privileges on protected endpoints in order to detect, block, and remediate threats that a standard user process cannot touch. On September 3, 2026, a security researcher operating under the handle Chaotic Eclipse (also known as Nightmare Eclipse, MSNightmare, and INFINITE NIGHTMARE) published a working proof-of-concept exploit to GitHub, naming it FalconFlank, that escalates a local, low-privileged Windows account to full SYSTEM privileges on a fully patched Windows 11 25H2 or Windows Server 2025 host running CrowdStrike Falcon [1][2][6]. The disclosure followed no coordinated timeline with CrowdStrike; the researcher's own GitHub notes anticipated that CrowdStrike would move quickly to add detections for the specific proof-of-concept, framing the release as intentionally adversarial toward the vendor [6].

This is not this researcher's first uncoordinated release against a major security vendor. According to reporting from Techzine, the same actor previously published exploits targeting Kaspersky and Microsoft Defender before turning attention to CrowdStrike Falcon, and has publicly criticized vendors' responsiveness to vulnerability reports as a stated motivation for skipping coordinated disclosure [5]. Security Affairs similarly notes that this researcher's prior releases against Microsoft Defender — including exploits it names Undefend and RedSun — have in some cases gone on to be exploited in the wild after public release [3]. CSA's AI Safety Initiative has separately analyzed a related pattern in a Microsoft Defender zero-day it tracks internally as RoguePlanet (CVE-2026-50656), disclosed by the same actor under the Nightmare Eclipse and Chaotic Eclipse aliases in June 2026, which similarly weaponized an antivirus engine's own privileged remediation pipeline to obtain SYSTEM access. FalconFlank extends that pattern to a second major EDR vendor, suggesting the technique class — abusing a security product's privileged file-remediation logic as a confused-deputy attack surface — is being deliberately and repeatedly targeted across the endpoint security market rather than arising as a one-off implementation bug.

CrowdStrike has stated it is "actively investigating these claims" and has published a FalconFlank Tech Alert to customers through its support portal, though that advisory is accessible only to authenticated CrowdStrike customers and is not a public document [1]. Publicly, the company has recommended a specific configuration change as an interim workaround while it evaluates the report, discussed in the Recommendations section below. As of this writing, CrowdStrike has not confirmed a CVE identifier, published a CVSS score, or announced a fix timeline.

Security Analysis

Technical Mechanism

FalconFlank targets Falcon's Microsoft Office File Suspicious Macro Removal capability, a remediation feature that inspects Office documents for malicious macros and, when Falcon's prevention policy is configured for "Phase 3 – Optimal Protection," automatically removes or neutralizes the offending content [1][3]. Because this remediation action must open, inspect, and rewrite file content that could otherwise carry a malicious macro, the component performing it necessarily operates with privileges well beyond those of the ordinary user account whose files are being remediated.

According to the researcher's public proof-of-concept and third-party technical write-ups, a low-privileged local process stages a specially crafted, OLE-formatted file – disguised so that Falcon's macro-scanning logic treats it as an Office document requiring remediation – in a location associated with the PowerShell version 1.0 application directory [4]. When Falcon's privileged remediation logic acts on that staged file, the attacker is able to cause a malicious library to land inside that trusted directory path, a location from which Windows will load DLLs (such as `bcrypt.dll`) into any process that subsequently invokes the PowerShell v1.0 runtime. The attacker then triggers execution in a manner that causes the planted library to be loaded in a privileged context, and the public PoC demonstrates the impact by spawning a command prompt running as NT AUTHORITY\SYSTEM [1][2]. CrowdStrike has not published its own technical analysis confirming or disputing this mechanism, so these details should be read as the best available third-party reconstruction rather than vendor-confirmed root cause; independent security researchers analyzing the public PoC broadly agree on the shape of the attack even without vendor confirmation [4].

The exploit's precondition – a security remediation feature that must operate with elevated privileges specifically because it handles untrusted file content – mirrors the exact structural flaw CSA documented in its internal analysis of the RoguePlanet Microsoft Defender zero-day: a privileged code path that exists to protect the endpoint becomes the vector by which the endpoint is compromised.

Scope and Affected Configurations

Confirmed affected configurations include Windows 11 (25H2 build) and Windows Server 2025 running CrowdStrike Falcon with a prevention policy set to "Phase 3 – Optimal Protection" and with the Microsoft Office File Suspicious Macro Removal setting enabled [1][3]. Because this remediation feature is a configurable policy option rather than a mandatory default in every Falcon deployment, exposure is not uniform: organizations that have not enabled this specific macro-removal setting, or that run an

earlier Falcon prevention policy tier, may not be exploitable through this particular path, though this has not been independently verified by CrowdStrike. Security teams should treat their own Falcon policy console, not vendor guidance alone, as the authoritative source for whether this configuration is active in their environment.

Exploitation Risk Assessment

FalconFlank is a local privilege escalation vulnerability, not a remote code execution vector — successful exploitation requires an attacker to already have code execution or interactive access as a standard user on the target endpoint. That precondition limits FalconFlank's utility as an initial-access technique, but it is highly valuable in the later stages of an intrusion: an attacker who has already achieved a foothold through phishing, a compromised credential, or a vulnerable third-party application can use FalconFlank to escalate to SYSTEM, disable or blind further Falcon telemetry, dump credentials, and move laterally with a trust level the endpoint's own security software was meant to deny them.

The absence of a CVE identifier or CVSS score complicates prioritization for organizations that route vulnerability response through formal scoring thresholds, and security teams should not wait for a CVE to be assigned before acting on the interim guidance below. No public reporting as of this writing confirms in-the-wild exploitation of FalconFlank specifically, and CrowdStrike has not issued a statement to that effect either way. However, the disclosing actor's track record — with prior Microsoft Defender exploits from the same aliases reportedly moving from proof-of-concept to observed use in a matter of weeks — argues against treating this as a low-urgency finding simply because it has not yet been weaponized [3].

Recommendations

Immediate Actions

Security teams running CrowdStrike Falcon should immediately audit their prevention policy configuration to determine whether the Microsoft Office File Suspicious Macro Removal setting is enabled and whether affected endpoints are configured for Phase 3 — Optimal Protection. Where the setting is enabled and not required for a specific business reason, CrowdStrike's own interim guidance — disabling the Microsoft Office File Suspicious Macro Removal Windows policy setting — should be applied, with the understanding that endpoints remain protected against malicious Office macros through Falcon's separate Cloud Anti-malware for Microsoft Office Files capability [1][5]. Organizations

with an active CrowdStrike support relationship should retrieve and review the FalconFlank Tech Alert published to the CrowdStrike support portal, since that advisory may contain detection content and configuration guidance beyond what has been made public.

Threat hunting teams should search endpoint telemetry, since the public proof-of-concept became available on September 3, 2026, for unexplained library files — particularly files resembling `bcrypt.dll` or other system libraries — written to the PowerShell v1.0 application directory, and for SYSTEM-context process creation events that do not correspond to expected administrative activity [4]. Given that the researcher explicitly anticipated CrowdStrike shipping signature-based detections for the public PoC, defenders should favor behavioral indicators of this kind over reliance on any single detection signature, since published exploit code is trivially modified and signature-only detection is a weak control against any actor who publishes source.

Short-Term Mitigations

While awaiting a vendor patch or CVE assignment, organizations should enforce least-privilege access on endpoints to reduce the population of accounts capable of the local code execution FalconFlank requires as a prerequisite. Application control or allowlisting policies that restrict which binaries may be written to or executed from application-specific directories such as the PowerShell v1.0 path add a layer of defense that does not depend on Falcon-specific remediation logic. Security teams should also confirm that Falcon sensor telemetry continues reporting normally on all endpoints, since an attacker who successfully escalates to SYSTEM may attempt to tamper with or blind the very sensor that failed to prevent the escalation.

Organizations should subscribe to CrowdStrike's advisory channels and support portal for updates on FalconFlank, and should plan to apply any forthcoming patch or configuration guidance on an expedited basis rather than the standard patch cycle, given the public availability of working exploit code and the disclosing actor's history of rapid weaponization of prior releases.

Strategic Considerations

FalconFlank is the second disclosed case within a few months in which the same threat actor has demonstrated that an endpoint security product's own privileged remediation logic can be turned into a SYSTEM-level privilege escalation primitive, following the RoguePlanet Defender disclosure in June 2026. Security leaders should treat this as evidence of a recurring vulnerability class — not a vendor-specific defect — and ask their own EDR and antivirus vendors, regardless of brand, how privileged remediation and quarantine code paths are isolated from the untrusted file content they process. Any

security product that must open, inspect, and act on attacker-influenced files with elevated privileges carries structurally similar risk, and procurement and architecture review processes should treat that question as a standing due-diligence item rather than a one-time evaluation.

The disclosure pattern itself is also strategically relevant. An actor who has stated frustration with vendor responsiveness as motivation for skipping coordinated disclosure [5] and who releases working exploits against multiple major security vendors without coordinated disclosure timelines represents a standing risk factor independent of any single vulnerability's technical merits. Organizations that depend on "wait for the vendor patch" as their primary posture toward zero-day disclosures are structurally exposed to this actor's disclosure model, and should weight investment in behavioral detection, least-privilege architecture, and endpoint telemetry integrity accordingly, rather than treating each new disclosure from this actor as an isolated emergency.

CSA Resource Alignment

FalconFlank connects directly to prior CSA AI Safety Initiative research and to CSA's broader control frameworks.

CSA's AI Safety Initiative has previously analyzed the identical structural flaw in internal research on RoguePlanet (CVE-2026-50656): an earlier disclosure by the same threat actor exploiting a security engine's privileged remediation pipeline to gain SYSTEM access, in that case against Microsoft Defender rather than CrowdStrike Falcon. The architectural lesson, exploitation risk framing, and behavioral-detection-over-signature guidance developed for that analysis apply with minimal modification to FalconFlank, and organizations that implemented the earlier recommendations are better positioned to extend equivalent monitoring to Falcon.

Separate internal CSA analysis of GentleKiller, the Gentlemen ransomware-as-a-service EDR-killer suite, reinforces the broader theme that endpoint security agents are themselves a high-value attack surface, though through a different mechanism (kernel driver abuse rather than remediation-pipeline abuse). Read together, that analysis and this note establish that both the kernel-mode and privileged-remediation layers of modern EDR platforms face active, demonstrated attack techniques, and defenders should not treat EDR deployment itself as a terminal control without additional layered defenses.

The CSA AI Controls Matrix (AICM) v1.1, available at cloudsecurityalliance.org/artifacts/ai-controls-matrix-v1-1, provides Threat & Vulnerability Management domain controls that apply directly to the compensating-control documentation organizations need while no patch or CVE exists for FalconFlank. Although AICM is scoped to AI system governance, its vulnerability management and least-privilege

control objectives are directly transferable to the endpoint security context described here, and organizations already using AICM as their governance baseline should extend its TVM domain controls to cover this disclosure pending a vendor fix.

References

[1] Sergiu Gatlan. "New CrowdStrike 'FalconFlank' zero-day grants SYSTEM privileges." BleepingComputer, September 4, 2026.

[2] Ravie Lakshmanan. "Researcher Releases FalconFlank PoC Showing Privilege Escalation in CrowdStrike Falcon." The Hacker News, September 3, 2026.

[3] Pierluigi Paganini. "Chaotic Eclipse Releases Crowdstrike Falcon ZeroDay FalconFlank." Security Affairs, September 3, 2026.

[4] Abstract Security. "Chaotic Eclipse Releases CrowdStrike Falcon Zero-Day FalconFlank: Detection Guidance." Abstract Security Blog, September 3, 2026.

[5] Erik van Klinken. "FalconFlank exposes CrowdStrike Falcon privilege flaw." Techzine Global, September 4, 2026.

[6] MSNightmare. "FalconFlank: Crowdstrike Falcon 0day Privilege Escalation Vulnerability." GitHub, September 3, 2026.