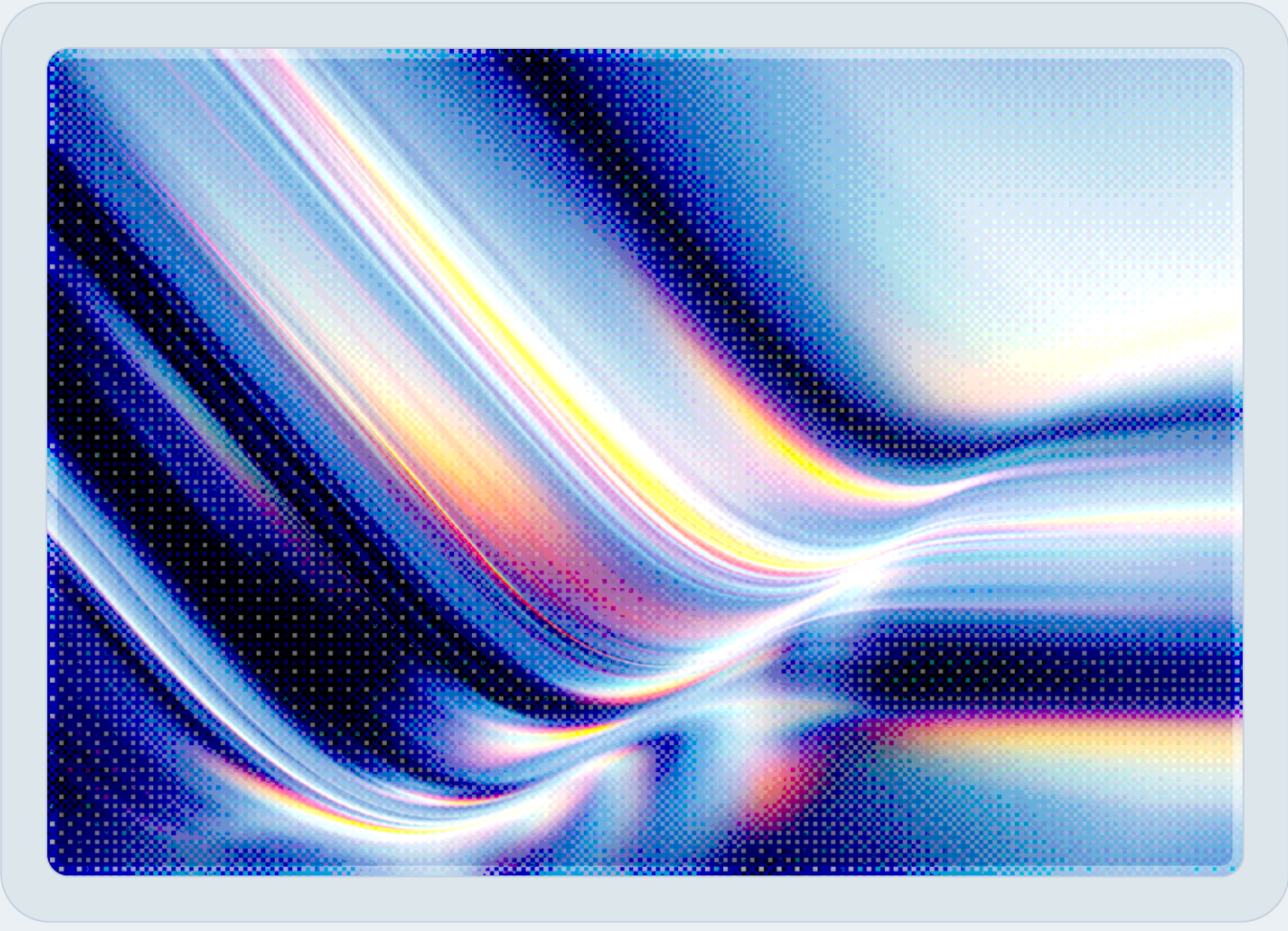
CSAI Foundation | Cloud Security Alliance

NVIDIA GreenSection: Unpatched GPU Driver Flaw Gets Public Exploit

A Researcher's Uncoordinated Disclosure Pattern Reaches NVIDIA While the Vendor Investigates

2026-09-09

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

- A researcher operating under the handle Chaotic Eclipse (also known as Nightmare Eclipse, Infinite Nightmare, and MSNightmare) published a working proof-of-concept for an unpatched NVIDIA GPU driver flaw, dubbed GreenSection, on or around September 7, 2026, while NVIDIA was still investigating the report and had not yet issued a fix or assigned a CVE identifier [1][3].
- GreenSection stems from a globally accessible shared memory section that multiple NVIDIA Windows user-mode driver components read from and write to with full permissions for any local user, and reused, insufficiently validated data from that section can trigger an out-of-bounds memory write [1]. NVIDIA has publicly acknowledged the report, stating it is "aware of reports describing a proof-of-concept that demonstrates improper access controls on a shared memory section used by certain NVIDIA GPU display driver components on Windows" [2][3].
- The public PoC reliably crashes applications that use the Vulkan or OpenGL graphics APIs but has not been shown to achieve SYSTEM-level privilege escalation [1][3]. The researcher has theorized, without demonstrating, that the underlying memory corruption could be abused to cross user-session boundaries or influence the Windows Desktop Window Manager process (`dwm.exe`) [1][3].
- GreenSection is one of at least four zero-days the same researcher released against non-Microsoft vendors in the final days of August and first two weeks of September 2026, alongside FalconFlank (CrowdStrike Falcon Sensor), PrettyPrague (Gen Digital's Avast/AVG/Norton products), and HardBreacher (Kaspersky), each disclosed without vendor coordination and each currently at a different stage of remediation [2][3].
- The disclosure extends a pattern CSA has tracked since this researcher's June 2026 release of the RoguePlanet Microsoft Defender exploit, in which functional, unpatched exploit code reaches the public internet before, or entirely without, a corresponding vendor advisory, substantially shortening defenders' effective response window and shifting the burden of interim risk assessment onto downstream security and IT teams [2][5].

Background

On September 7, 2026, Security Affairs and the German technology outlet igor'sLAB reported that a security researcher publishing under the aliases Chaotic Eclipse, Nightmare Eclipse, Infinite Nightmare, and MSNightmare had released a public proof-of-concept exploit for a previously undisclosed NVIDIA GPU driver vulnerability [1][3]. The researcher named the flaw GreenSection, continuing a naming convention used across their prior disclosures. NVIDIA had not shipped a patch and had not assigned a CVE identifier as of publication, which left organizations running the affected driver components without a vendor-supplied timeline for remediation, and with only the researcher's own technical write-up to assess their exposure [1][3][4].

GreenSection did not arrive in isolation. SecurityWeek reported that the same researcher released GreenSection alongside two other zero-days -- FalconFlank, targeting CrowdStrike's Falcon Sensor, and PrettyPrague, targeting Gen Digital's Avast antivirus sandbox -- in a tight window spanning late August and early September 2026 [2]. These followed an earlier release, HardBreacher, against Kaspersky endpoint security software, which Kaspersky addressed through an automatic signature-database update on August 31, 2026 [2]. Independent security researcher Kevin Beaumont confirmed that the Avast, CrowdStrike, and Kaspersky proofs-of-concept were functional, lending credibility to the researcher's broader run of disclosures, even where individual vendors have disputed severity or scope [2].

The researcher's history predates this cluster of releases. Before turning attention to security vendors and NVIDIA, Chaotic Eclipse built a reputation releasing zero-day exploits against Microsoft products, including the BlueHammer flaw tracked as CVE-2026-33825 and, most notably for CSA's prior coverage, the RoguePlanet privilege-escalation exploit against Microsoft Defender, tracked as CVE-2026-50656 [5]. In that case, a functional public exploit circulated for roughly a week before Microsoft assigned a CVE and confirmed the issue, illustrating the same core dynamic now playing out with NVIDIA: uncoordinated release of working exploit code that forces vendors into public investigation mode rather than a private, scheduled remediation process [5]. The researcher has been open about the motivation behind this approach, telling reporters that they view established vendors' engagement with independent researchers -- particularly Microsoft's -- as inadequate, and has expressed frustration that vendors characterize the disclosures as reckless rather than engaging with the underlying findings [2][4].

The shift toward targeting security and infrastructure vendors, rather than end-user operating system components, carries its own attack-surface implications. CrowdStrike, Gen Digital, and Kaspersky occupy privileged positions on the systems they protect, and NVIDIA's GPU drivers are ubiquitous across consumer, gaming, and, increasingly, AI training and inference infrastructure that depends on NVIDIA

hardware for compute. A flaw in a component that touches every user session on a Windows system running an NVIDIA GPU therefore has a large potential attack surface even before its exploitability ceiling is fully understood.

Security Analysis

The GreenSection Mechanism

According to the technical description carried by Security Affairs, GreenSection centers on a shared memory section, identified in the researcher's write-up as `\BaseNamedObjects\{52813408-3561-4705-820a-2b3b78be92ba}`, that multiple NVIDIA Windows user-mode driver components create and access with full read and write permissions granted to any local user [1]. The section is intended to hold data structures that support inter-process coordination among driver components, and NVIDIA's code includes runtime checks meant to validate that data before it is used. The vulnerability arises because those checks are insufficient in at least one code path: data read back from the shared section can be reused in a way that drives an out-of-bounds memory write, corrupting adjacent memory rather than being safely rejected [1].

In its current public form, the exploit reliably crashes applications built on the Vulkan or OpenGL graphics APIs, which is consistent with memory corruption inside a shared driver component that those APIs depend on [1][3]. The researcher has not demonstrated a working path to SYSTEM-level privilege escalation, and igor'sLAB's independent write-up is explicit that "complete privilege escalation to the SYSTEM level" has not been shown [3]. What the researcher has put forward -- without a working demonstration -- is that the same memory corruption primitive could plausibly be extended to cross session or user boundaries, or to influence the Desktop Window Manager process that composites the desktop for every logged-in user [1][3]. Readers should treat this extension as an informed hypothesis from someone with direct knowledge of the bug rather than a confirmed capability; the distance between "corrupts memory in a shared driver section" and "reliable, weaponizable privilege escalation across the Windows security boundary" can be substantial and NVIDIA's own investigation may narrow or widen that gap once it concludes.

NVIDIA's public response so far consists of an acknowledgment and a statement that it is investigating. The company stated it is "aware of reports describing a proof-of-concept that demonstrates improper access controls on a shared memory section used by certain NVIDIA GPU display driver components on Windows" [2][3]. As of this note's publication, NVIDIA has not confirmed which driver branches or GPU

product lines are affected, has not published a security bulletin, and has not assigned a CVE identifier, which leaves security teams without an authoritative severity rating or a defined scope of affected driver versions.

Part of a Broader Disclosure Pattern

GreenSection is best understood in the context of the other disclosures the same researcher released in the same window. The following table summarizes the four most recent releases and their remediation status as of this note's publication.

Codename	Target	Reported Impact	CVE Assigned	Patch Status (as of Sept. 9, 2026)
HardBreacher	Kaspersky endpoint security	Local privilege escalation	Not disclosed	Fixed via automatic signature-database update, August 31, 2026 [2]
PrettyPrague	Gen Digital Avast (and potentially AVG, Norton) sandbox	Privilege escalation to full-system shell	Not disclosed	Fixed; Gen Digital shipped versions 26.7.11086 and 26.8.11125, September 4, 2026 [2][3]
FalconFlank	CrowdStrike Falcon Sensor (Office macro remediation feature)	Local privilege escalation to SYSTEM on fully patched Windows 11 25H2 / Server 2025	Not disclosed	Unpatched; CrowdStrike recommends temporarily disabling the affected policy setting [2][3][4]
GreenSection	NVIDIA Windows GPU display driver components	Memory corruption; application crashes; unconfirmed cross-boundary risk	Not assigned	Unpatched; NVIDIA investigating [1][3][4]

Two patterns stand out. First, remediation speed appears linked to how directly a vendor's existing update mechanism can absorb the fix, though the sample here is small (four disclosures): Kaspersky and Gen Digital, which can push signature or application updates on short cycles, closed their respective issues within days, while CrowdStrike and NVIDIA, whose fixes likely require more deliberate driver or agent engineering changes, remain in an investigation-and-workaround posture [2][3]. Second, none of the four disclosures followed a coordinated vulnerability disclosure timeline in which the vendor has an opportunity to patch before public release. That absence of coordination is a deliberate choice by the researcher, consistent with the approach documented in CSA's earlier RoguePlanet research note, and it suggests defenders should plan on this researcher's future disclosures arriving with working exploit code already public, rather than as advance notice, though this pattern could change [5].

Risk Assessment for GreenSection Specifically

Absent a CVE and an NVIDIA security bulletin, organizations cannot yet rely on a CVSS score to prioritize GreenSection. Based on the publicly available technical details, CSA's interim assessment is that the demonstrated impact -- denial of service against graphics-API applications -- is disruptive but would not, on its own, warrant a high-severity rating; this assessment may change once NVIDIA publishes a bulletin. The undemonstrated potential for cross-user or `dwm.exe` compromise is the detail that warrants monitoring rather than immediate alarm: if NVIDIA's investigation or independent researchers confirm a path to privilege escalation or lateral movement across user sessions, the risk profile would shift substantially, particularly for shared or multi-user Windows systems such as virtual desktop infrastructure, GPU-accelerated cloud workstations, and shared AI development environments where multiple users or workloads rely on the same physical GPU and driver stack. Organizations operating such shared-GPU environments should treat GreenSection as a flaw to track closely rather than one to dismiss because a full exploit chain has not yet been published.

Recommendations

Immediate Actions

Security teams should inventory which endpoints and servers run affected NVIDIA GPU drivers, with particular attention to shared or multi-tenant systems such as virtual desktop infrastructure, GPU-accelerated development workstations, and cloud-hosted AI training or inference environments where several users or processes share a single GPU. Because NVIDIA has not yet published an affected-versions list, teams cannot narrow this inventory by driver version alone and should instead treat any Windows system with an NVIDIA GPU as potentially in scope until NVIDIA's bulletin clarifies the

boundary [1][3]. Teams should also subscribe to NVIDIA's product security page and enable notifications so that a forthcoming driver update or advisory reaches the right owners immediately, and should apply the same tracking discipline to FalconFlank if CrowdStrike Falcon Sensor is deployed, since that exploit also remains unpatched [2][4].

Short-Term Mitigations

Until NVIDIA ships a fix, organizations should prioritize monitoring over speculative workarounds, since no vendor-endorsed mitigation for GreenSection has been published and no configuration change is known to close the underlying shared-memory permission gap. Endpoint detection and response tooling should be tuned to flag anomalous crashes in Vulkan- or OpenGL-based applications correlated with unexpected process behavior, since that is the only reliably observable symptom documented in public reporting so far [1]. Organizations running shared-GPU virtual desktop or cloud AI infrastructure should reduce the practical impact of an unproven cross-user escalation by reinforcing session isolation and least-privilege configuration on those hosts now, rather than waiting for confirmation that such an escalation path exists. For the CrowdStrike FalconFlank exploit, security teams should follow CrowdStrike's guidance to temporarily disable the affected Microsoft Office File Suspicious Macro Removal policy setting while relying on other Falcon protections to cover the resulting gap [2][3].

Strategic Considerations

This disclosure reinforces a lesson CSA drew from the RoguePlanet Microsoft Defender case: when a researcher operates outside coordinated disclosure norms, as this one has repeatedly done, organizations cannot assume a meaningful gap will exist between a zero-day's public release and a vendor's confirmation or patch [5]. A single researcher operating outside coordinated disclosure norms has now produced functional exploit code against Microsoft, Kaspersky, Gen Digital, CrowdStrike, and NVIDIA within roughly six months, spanning operating system, endpoint security, and hardware driver layers. Security leaders should treat this as evidence that vulnerability management programs need a standing process for triaging vendor-unconfirmed, CVE-less reports from credible independent researchers, rather than waiting for the formal advisory pipeline that this researcher has repeatedly chosen to bypass. Organizations with significant GPU-dependent infrastructure -- including AI training and inference environments that increasingly run multi-tenant workloads on shared NVIDIA hardware -- should also use this incident to reassess whether GPU driver components are adequately covered by existing vulnerability management and patch-testing processes, which may have historically focused more heavily on operating systems and endpoint agents than on graphics driver stacks.

CSA Resource Alignment

CSA's June 2026 research note on RoguePlanet, the Microsoft Defender zero-day tracked as CVE-2026-50656, is the most directly applicable prior CSA artifact to this disclosure, since it documents the same researcher's uncoordinated disclosure methodology and provides a detailed template for triaging an unpatched, publicly-exploited vulnerability before a vendor advisory exists [5]. The behavioral detection guidance, threat-actor profiling, and Threat and Vulnerability Management (TVM) domain mapping in that note apply with only minor adaptation to GreenSection: both cases involve a credible researcher publishing working exploit code against a vendor that has not yet confirmed scope or shipped a fix, and both require defenders to build interim detections around observable symptoms rather than a CVSS-scored, vendor-validated exploit chain.

CSA's research note on CitrixBleed Infinity, covering the rapid exploitation of the NetScaler memory-overread flaw tracked as CVE-2026-8451, is also relevant, though for a different reason: it documents how quickly a publicly disclosed memory-safety flaw moved from technical write-up to internet-wide scanning and exploitation, in that case within roughly 24 hours [6]. GreenSection has not yet reached that stage, and the absence of a confirmed privilege-escalation path may mean it never does, but the CitrixBleed Infinity note's recommendation that organizations shift toward Zero Trust architectures rather than relying solely on patch discipline for memory-safety-class vulnerabilities is directly applicable to GPU driver components that, like NetScaler, sit in a privileged position relative to the workloads and users around them.

More broadly, the CSA AI Controls Matrix (AICM) v1.1's Threat and Vulnerability Management domain provides the standing framework organizations should use to formalize the triage process this incident calls for: tracking unconfirmed, CVE-less vulnerability reports from credible external researchers, assigning interim risk ratings pending vendor confirmation, and documenting compensating controls until a patch is available [7]. AICM v1.1's Model Security domain and its broader coverage of AI infrastructure controls are also worth revisiting for organizations whose GPU fleets support AI training or inference workloads, since a driver-layer flaw in shared compute infrastructure sits upstream of the model and data protections that domain is designed to address [7].

References

[1] Paganini, P. "Chaotic Eclipse Released A PoC For NVIDIA GreenSection Memory Corruption Zero-Day." Security Affairs, September 7, 2026.

[2] SecurityWeek. "Nightmare Eclipse Drops CrowdStrike, Nvidia, Avast Zero-Day Exploits." SecurityWeek, September 2026.

[3] igor'sLAB. "Nightmare Eclipse: PoCs Targeting NVIDIA, CrowdStrike, and Avast -- Patch Status Varies." igor'sLAB, September 7, 2026.

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

[5] Cloud Security Alliance AI Safety Initiative. "RoguePlanet: Microsoft Defender Zero-Day CVE-2026-50656." CSA Lab Space, June 19, 2026.

[6] Cloud Security Alliance AI Safety Initiative. "CitrixBleed Infinity: NetScaler Flaw Exploited Within Hours." CSA Lab Space, July 4, 2026.

[7] Cloud Security Alliance. "AI Controls Matrix v1.1." CSA, June 22, 2026.

This research note provides point-in-time guidance as of 2026-09-09. NVIDIA's investigation is ongoing and may result in a security bulletin, CVE assignment, or driver update that supersedes elements of this analysis. Monitor NVIDIA's product security page and referenced sources for updates.

Document Classification: TLP:CLEAR - Unlimited distribution.