WHITE PAPER

CYTEX™

AI-Powered Resilience Command Center

MiniPlasma

A Five-Year-Old Windows Privilege Escalation Flaw

hello@cytex.io | https://cytex.io

© Cytex, Inc. All rights reserved.

MiniPlasma

Technical analysis of the Cloud Files Mini Filter Driver flaw resurrected with a working public exploit on May 14, 2026, by the same researcher behind YellowKey and GreenPlasma.

What Happened

On May 14, 2026, the researcher operating under the handles **Chaotic Eclipse** and **Nightmare-Eclipse** published a working proof-of-concept exploit for **CVE-2020-17103**, a local privilege escalation vulnerability in the Windows Cloud Files Mini Filter Driver (cldflt.sys). The flaw was originally reported to Microsoft in September 2020 by security researchers and assigned a CVE with a reported fix in December 2020.

The researcher's central claim: the original proof-of-concept from 2020 works on fully patched, current Windows systems without modification. Either Microsoft never actually fixed CVE-2020-17103, or the fix was silently reverted in a subsequent update.

This is the same researcher who released **BlueHammer** (CVE-2026-33825), **RedSun**, **UnDefend**, **YellowKey** (BitLocker bypass), and **GreenPlasma** (CTFMON privilege escalation) in 2026. MiniPlasma is the latest entry in a disclosure pattern timed deliberately around Microsoft's Patch Tuesday cycle, with each release PGP-signed for verifiable authorship continuity.

The release was accompanied by the researcher's public commentary that the disclosure pattern is intentional retaliation for Microsoft's handling of prior vulnerability submissions, and that further releases are planned for subsequent Patch Tuesdays.

Vulnerability Profile

Attribute	Detail
Name	MiniPlasma
CVE	CVE-2020-17103
Class	Local privilege escalation to SYSTEM
Affected component	cldflt.sys (Cloud Files Mini Filter Driver)
Affected routine	HsmOsBlockPlaceholderAccess
Exploitation primitive	Abuse of the undocumented CfAbortHydration API
Originally reported	September 2020
Reportedly fixed	December 2020
Current patch status	Public PoC works against fully patched modern Windows

Attribute	Detail
Affected platforms	Windows 10 and Windows 11 with Cloud Files enabled
Required access	Unprivileged local user account
Public PoC	Released May 14, 2026 on GitHub by Nightmare-Eclipse
New CVE assigned	None as of this writing
Microsoft response	None as of this writing

How MiniPlasma Works

The Cloud Files Mini Filter Driver

cldflt.sys is the kernel-mode component behind the **Cloud Files API**, the Windows subsystem that powers OneDrive Files On-Demand, third-party cloud sync providers, and any application that exposes "placeholder" files to the user. Placeholders look and behave like files on disk but are actually metadata stubs that trigger on-demand download (hydration) when accessed.

Because the driver mediates between user-mode applications and kernel-protected file-system state, it operates at high privilege and exposes a set of APIs that user-mode callers can invoke to manipulate placeholder state. Some of these APIs are documented. Others, including CfAbortHydration, are not.

The Original 2020 Defect

The 2020 disclosure identified that the HsmOsBlockPlaceholderAccess routine inside cldflt.sys performed insufficient access validation when handling certain placeholder operations. Specifically, the routine could be reached through the undocumented CfAbortHydration API in a way that allowed an unprivileged caller to influence operations performed against registry keys in the **.DEFAULT user hive**.

The .DEFAULT hive is the registry profile used by the SYSTEM account and processes running before any user logs in. Write access to .DEFAULT is effectively write access to SYSTEM-context configuration. The 2020 PoC demonstrated arbitrary registry key creation in .DEFAULT without the access checks that should have prevented it, providing the primitive needed for SYSTEM privilege escalation.

The Exploit Chain

Reconstructing the chain from the published PoC and the original 2020 advisory:

Step 1. An unprivileged user-mode process invokes the undocumented CfAbortHydration API with crafted arguments against a Cloud Files placeholder under attacker control.

Step 2. The call routes into cldflt.sys and reaches the HsmOsBlockPlaceholderAccess routine. The routine fails to validate that the calling context is authorized to perform the resulting downstream operations.

Step 3. The routine performs registry operations that ultimately allow the attacker to create arbitrary keys inside the .DEFAULT hive, an operation that should require SYSTEM-level access.

Step 4. The attacker plants registry content under .DEFAULT that influences the loading or behavior of a SYSTEM-context process. Common patterns include staging a malicious DLL path that a SYSTEM service will load, or modifying configuration values consumed by a privileged process at next invocation.

Step 5. The SYSTEM-context process loads the attacker-controlled content. Code executes at SYSTEM privilege.

Why This Exploit Class Is Hard to Detect

Three properties of MiniPlasma make it operationally stealthier than typical kernel privilege escalations:

The exploit uses **documented and undocumented Microsoft APIs** rather than memory corruption or shellcode. There is no buffer overflow, no ROP chain, no payload that resembles malware. The system calls being made are legitimate kernel interfaces.

The exploit relies on **cldflt.sys**, a driver loaded on virtually every modern Windows installation by default. There is no rare component to flag. The driver's normal operation involves heavy interaction with the file system, the registry, and user-mode applications.

The privilege escalation occurs through **registry writes**, which are routine across millions of legitimate Windows operations per hour on a typical endpoint. Distinguishing a malicious write to .DEFAULT from a legitimate one requires context about *who* wrote it and *why*, and most EDR products do not track that lineage with sufficient resolution.

The Patch Regression Question

The technically significant element of this disclosure is not the vulnerability itself. It is the claim that **the 2020 patch is no longer effective**. Two scenarios fit the available evidence:

Scenario one. The original December 2020 fix addressed a different code path than the one the PoC actually exercised, and the underlying defect in HsmOsBlockPlaceholderAccess was never closed. The 2020 advisory was marked resolved based on the surface-level remediation, but the primitive remained reachable through CfAbortHydration.

Scenario two. The original fix was correct in December 2020 but was reverted or regressed in a subsequent Windows update. Driver-level code changes in cldflt.sys between 2020 and 2026 could have re-introduced the defect inadvertently. This pattern, where a security fix is undone by later refactoring, has precedent in other long-lived Windows components.

Independent verification of which scenario applies requires comparative analysis of cldflt.sys binaries from the December 2020 patched build, intermediate builds, and the current build. That analysis has not yet been publicly published. Either scenario carries the same defensive implication: **CVE-2020-17103 is currently exploitable on fully patched Windows systems**, and the original PoC from 2020 reportedly works without modification.

The broader pattern is concerning beyond this specific CVE. If a high-severity privilege escalation patched in 2020 is exploitable again in 2026, the same possibility applies to other historical Windows kernel-driver vulnerabilities. Defensive programs should not assume that "patched five years ago" means "still patched today" for components that have undergone significant refactoring in the interim.

Affected Systems

MiniPlasma affects Windows installations where the **Cloud Files Mini Filter Driver is loaded and active**. This includes:

- Windows 10 and Windows 11 client systems with OneDrive or other Cloud Files API consumers installed
- Windows Server editions where Cloud Files functionality is enabled
- Default Windows installations on most modern hardware, since cldflt.sys is registered by default even when OneDrive is not actively syncing

Systems where the driver is explicitly disabled or removed are not exploitable through the published PoC. In practice, this excludes a small fraction of enterprise endpoints, since the driver is rarely uninstalled in standard configurations.

Detection Signals

There are no traditional malware IOCs for MiniPlasma. The exploitation uses legitimate Windows kernel interfaces. Detection is behavioral, focused on the specific patterns the PoC and likely derivative exploits will produce.

Registry-level signals:

- Creation of registry keys or values inside HKEY_USERS\.DEFAULT by processes that are not legitimately operating in SYSTEM context
- Modifications to subkeys under .DEFAULT that influence DLL load paths, service configuration, or scheduled task definitions, originating from user-context processes
- Sequences of registry writes to .DEFAULT correlated with prior cldflt.sys activity from the same process

Driver and API signals:

- Calls into cldflt.sys from processes that have no legitimate cloud sync role, particularly invocations of placeholder lifecycle APIs from short-lived or non-cloud-aware processes
- High-frequency invocation of placeholder hydration and abort operations against attacker-controllable file paths
- Unusual interactions with directories used for OneDrive or other Cloud Files providers from processes that are not the registered provider

Process telemetry signals:

- Unexpected SYSTEM-context process creation shortly after a sequence of user-context placeholder API calls
- DLLs loaded into SYSTEM-context processes from paths recently written to by unprivileged processes
- New scheduled tasks or services created in SYSTEM context with no corresponding administrative session

Threat intelligence signals:

- File hashes of the published Nightmare-Eclipse PoC artifacts, available from the GitHub repository, should be added to enterprise threat intelligence feeds for retrospective hunting
- Monitoring of the Nightmare-Eclipse GitHub account for additional disclosures tied to the same campaign

Sysmon coverage focused on registry events under .DEFAULT and image-load events for cldflt.sys-adjacent processes provides the strongest detection foundation. Most EDR products do not flag these events by default. Custom rules are required.

Defensive Actions

Until a confirmed patch is released, the following compensating controls apply.

Disable the Cloud Files Mini Filter Driver on critical infrastructure. On servers and high-value endpoints where Cloud Files functionality is not required, the driver can be disabled through filter driver management. This eliminates the attack surface entirely on those systems but breaks OneDrive Files On-Demand and any third-party Cloud Files provider. Apply only where the operational impact is acceptable.

The driver can be disabled administratively:

fltmc unload cldflt

sc config cldflt start= disabled

Verify operational dependencies before applying broadly. Roll out to critical infrastructure first, then to general endpoints only after impact assessment.

Apply least-privilege controls aggressively. MiniPlasma requires an unprivileged local foothold to escalate. Any control that prevents the initial foothold also prevents the privilege escalation. Application allowlisting, browser exploitation defenses, phishing protection, and macro execution policies all reduce the population of code paths that can reach the exploit.

Instrument Sysmon for .DEFAULT registry activity and cldflt.sys interactions. This is the detection foundation that compensates for the absence of EDR coverage. Forward Sysmon registry events under HKEY_USERS\.DEFAULT to the SIEM with correlation rules that flag user-context writes.

Audit current cldflt.sys version across the fleet. Identify which build is deployed where. When Microsoft releases a fix, comparative analysis of pre-fix and post-fix binaries will determine which systems were exposed during the open window. This audit data has forensic value regardless of patch timing.

Plan for the next disclosure. The researcher has publicly committed to additional releases at subsequent Patch Tuesdays. Defensive programs should treat the Patch Tuesday window as adversarially scheduled. Out-of-band response procedures, compensating controls, and detection rules should be staged in advance of the next disclosure cycle.

Treat historical CVEs as potentially live. MiniPlasma is the first publicly demonstrated case in 2026 of a years-old Windows CVE being weaponized through an unmodified original PoC. It is unlikely to be the last. Threat intelligence and red-team programs should periodically retest historical PoCs against current builds for high-impact CVEs in kernel-mode components that have undergone significant refactoring.

What This Disclosure Reveals About Patch Trust

The defensive assumption underlying most enterprise vulnerability management is that **a CVE marked "patched" stays patched**. MiniPlasma directly contradicts that assumption for at least one high-severity Windows kernel-driver vulnerability. The implications extend beyond CVE-2020-17103:

The patch lifecycle is **not monotonic**. Code changes in long-lived components can re-introduce previously fixed defects, and the systems that track CVE remediation status do not, in general, re-verify fixes against the current build of the affected component.

The cost of **historical exploit weaponization** is now low. The researcher did not develop a new exploit. The 2020 PoC was reused without modification. Any threat actor with access to historical PoC code can attempt the same revalidation against current Windows builds at minimal cost.

The defensive program needs to **periodically retest** rather than trust the patch ledger. For high-severity kernel-mode CVEs that touch components under active refactoring, point-in-time fix verification is insufficient. Continuous validation, either through internal red-team exercises or

through threat intelligence feeds that monitor for resurrected vulnerabilities, becomes part of the defensive baseline.

The disclosure pattern of the **same researcher releasing escalating exploits on a committed schedule** introduces an adversarial component to the patch cycle that traditional vulnerability management programs are not structured to handle. The next disclosure is announced. The cadence is committed to publicly. Defensive programs that calibrate to monthly patch rhythms will be exposed during each release window.

Sources

- Original 2020 advisory: CVE-2020-17103, Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
- Microsoft Security Response Center disclosure history for CVE-2020-17103
- Original 2020 PoC by Google Project Zero researchers, archived in Project Zero issue tracker
- Nightmare-Eclipse GitHub repository, PGP-signed disclosure post, May 14, 2026

Ready to see how AICenturion can secure you against AI risks?

Request a demo today: hello@cytex.io