VULNERABILITY BULLETINS

Microsoft Windows Cloud Files Minifilter Privilege Escalation Vulnerability (CVE-2025-55680)

TLP:WHITE

Oct 30, 2025

In March 2024, Exodus Intelligence discovered a vulnerability in Microsoft Windows Cloud Files Minifilter driver. The patch for this flaw was recently released, included in Microsoft's October 2025 Patch Tuesday, and is tracked as CVE-2025-55680.

The flaw is considered critical with a CVSS score of 7.8, which is a race condition vulnerability in the said driver, allowing threat actors to elevate privileges and create arbitrary files on systems when exploited.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

A vulnerability in Microsoft Windows Cloud Files Minifilter driver, tracked as CVE-2025-55680 (CVSS score of 7.8), was initially discovered by Exodus Intelligence in March 2024. Recently, Microsoft released a patch for this vulnerability as part of their October 2025 Patch Tuesday.

Microsoft Windows Cloud Files Minifilter is a type of file system filter driver that acts as a proxy between applications and a cloud sync engine, managing files stored in the cloud.

The flaw occurs due to a Time-of-Check Time-of-Use (TOCTOU) race condition in the specified driver, allowing a low-privileged, local attacker to exploit this kernel-mode flaw for privilege escalation to SYSTEM-level by creating arbitrary files in privileged locations, potentially enabling DLL side-loading.

There have been no known in-the-wild exploitations of this vulnerability.

The vulnerability affects multiple versions of Microsoft Windows operating systems, including:

- Windows 11 (versions 22H2, 23H2, 24H2, and 25H2)
- Windows 10 (versions 21H2 and 22H2, as well as version 1809)
- Windows Server 2022
- Windows Server 2019
- Windows Server 2025 (pre-release version)

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Prioritize patching and conduct a risk assessment for your systems.
- Enforce strict Least Privilege (Zero Trust) by implementing Role-Based Access Controls (RBAC) and Application Control.
- Employ secure network segmentation.

- Leverage advanced Endpoint Detection and Response (EDR).
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	exodusintel, hhs, microsoft, cybersecuritynews

Alert ID c197d463

View Alert

Share Feedback

was this helpful?  | 

Tags Microsoft Windows Cloud Files Minifilter, CVE-2025-55680, race condition, Arbitrary File, Microsoft, Privilege Escalation

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**