EnCyb

Severity: High

Advisory Type: Security

OneDrive Hijacking Vulnerability

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Security researchers and incident responders are observing active abuse of Microsoft OneDrive binaries (e.g., OneDrive.exe / OneDriveUpdater.exe) to perform DLL side-loading: attackers place a malicious DLL beside a trusted OneDrive binary (or otherwise influence the DLL search path) so Windows loads the attacker's DLL and executes malicious code in the context of a signed/legitimate process. This technique enables stealthy code execution, persistence, and defense evasion and has been observed in cryptojacking and broader intrusion activity.

- Vulnerability: DLL vulnerability
- Affected Sector: All sectors using Microsoft OneDrive in Windows environments
- Affected Product: Microsoft OneDrive / OneDriveUpdater
- Severity: High
- Published Date: Nov 05, 2025

TECHNICAL DETAILS

- Attacker obtains write access to a folder that will be searched by the OneDrive binary at load time (for example, user profile folders, mounted drives, or the same directory as the executable) and drops a malicious DLL whose name matches a legitimately resolved import.
- **Trigger / execution:** When OneDrive.exe / OneDriveUpdater.exe starts or when the updater runs, Windows loader resolves imports and loads the malicious DLL instead of the expected system DLL. The malicious DLL runs inside the OneDrive process.
- **Post-execution activity:** The DLL may spawn child processes, drop additional payloads, reach out to C2, install persistence artifacts, harvest credentials, or install coinminers/backdoors. Historic campaigns used this for cryptojacking and backdoor persistence.
- **Evasion:** Execution under a signed Microsoft binary reduces suspiciousness in many monitoring systems and may bypass poorly configured allowlists/AV detections**.**

IMPACT

- Arbitrary code execution inside a trusted, signed process.
- Stealthy persistence and reduced detection due to legitimate binary usage.
- Potential privilege escalation and lateral movement from compromised host.
- Delivery of payloads: backdoors, ransomware, cryptominers.
- Operational disruption, remediation cost, regulatory damage and reputational loss.
- Access to or exfiltration of user/cloud data, and file integrity tampering.

RECOMMENDATIONS

- Prevent arbitrary file writes to folders where signed binaries reside; restrict write access to user profile directories used by signed apps Implement **allow-lists** for trusted packages only.
- Reduce local admin rights; educate users and admins about safe file sharing and the risk of mounting untrusted images (attackers often use mounted media or sync folders to place DLLs).
- Delete malicious DLL files found in OneDrive/Teams/sync directories and any dropped payloads. Note that simple removal may not remove persistence.
- If credential theft or lateral movement is suspected, rotate impacted user/service credentials and revoke sessions/tokens.

REFERENCES

- https://gbhackers.com/hackers-abuse-onedrive-exe-via-dll-sideloading/
- https://cyberpress.org/onedrive-exe-execute-malicious-code/
- https://www.redhotcyber.com/en/post/danger-for-onedrive-users-infected-dlls-hide-in-shared-files/e-encryption/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com