Alerts

Vulnerability in Windows File System Proxy (WinFsp)

27 April 2026

CSA has issued a CVE ID to a vulnerability reported in WinFsp as part of CSA's Responsibility Vulnerability Disclosure Policy. Users and administrators of the affected product version are advised to update to the latest version immediately.

Background

CSA has issued a CVE ID (CVE-2026-3006) to a vulnerability reported in WinFsp, an open-source system software. The Product Owner of WinFsp has released a security update to address it.

Impact

Successful exploitation of the race condition vulnerability could allow an attacker to trigger a kernel heap overflow, potentially leading to local privilege escalation and granting system-level access to the affected software.

Affected Products

The vulnerability affects WinFsp versions 2.1.25156 and lower.

Mitigation

Users and administrators of affected product versions are advised to update to the latest version immediately.

Special Thanks to:

- Informer: Mr Tay Kiat Loong
- Product Owner: WinFsp

References

https://github.com/winfsp/winfsp/releases/tag/v2.2B1 ↗

↑ Back to top