Race Condition Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-3006
State	PUBLISHED
Assigner	CSA
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 03:15:59 UTC
Updated	2026-04-27 14:16:47 UTC
Description	Successful exploitation of the race condition vulnerability could allow an attacker to trigger a kernel heap overflow, potential

Risk And Classification

Primary CVSS: v3.1 7 HIGH from 5f57b9bf-260d-4433-bf07-b6a79e9bb7d4

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-362 | CWE-362 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	Secondary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WinFSP	WinFSP	affected 2.1.25156 and lower	Not specified

References

Reference	Source	Link	Tags
github.com/winfsp/winfsp/releases/tag/v2.2B1	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	github.com	
www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-043	5f57b9bf-260d-4433-bf07-b6a79e9bb7d4	www.csa.gov.sg	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Tay Kiat Loong (en)

Additional Advisory Data

Solutions

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

There are currently no legacy QID mappings associated with this CVE.