



# Race Condition Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-3006
<b>State</b>	PUBLISHED
<b>Assigner</b>	CSA
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 03:15:59 UTC
<b>Updated</b>	2026-04-27 14:16:47 UTC
<b>Description</b>	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	<b>CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</b>
3.1	CNA	CVSS	7	HIGH	<b>CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</b>

## 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	<a href="#">WinFSP</a>	<a href="#">WinFSP</a>	affected 2.1.25156 and lower	Not specified

#### References

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)