



# Host Process for Windows Tasks Elevation of Privilege Vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-60710
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-11-11 18:15:39 UTC
<b>Updated</b>	2026-04-14 14:44:19 UTC
<b>Description</b>	Improper link resolution before file access ('link following') in Host Process for Windows Tasks allows an authorized attacker

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from secure@microsoft.com

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

**EPSS:** 0.179690000 probability, percentile 0.951660000 (date 2026-04-18)

**CISA KEV:** Listed on 2026-04-13; due 2026-04-27; ransomware use Unknown

**Problem Types:** CWE-59 | CWE-59 CWE-59: Improper Link Resolution Before File Access ('Link Following')

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Windows
<b>Name</b>	Microsoft Windows Link Following Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2025-60710">https://nvd.nist.gov/vuln/detail/CVE-2025-60710</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 11 24h2	All	All	All	All
Operating System	Microsoft	Windows 11 25h2	All	All	All	All
Operating System	Microsoft	Windows Server 2025	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Windows 11 Version 24H2	affected 10.0.26100.0 10.0.26100.7462 custom	ARM64-based Systems
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.7462 custom	Not specified
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.7462 custom	x64-based Systems
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.7462 custom	x64-based Systems

### References

Reference	Source	Link
<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710">msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710</a>	secure@microsoft.com	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710">msrc.microsoft.com</a>
<a href="https://www.vicarius.io/vsociety/posts/cve-2025-60710-mitigation-script-eop-vulnerability/">www.vicarius.io/vsociety/posts/cve-2025-60710-mitigation-script-eop-vulnerability/</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.vicarius.io/vsociety/posts/cve-2025-60710-mitigation-script-eop-vulnerability/">www.vicarius.io</a>
<a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov</a>
<a href="https://www.vicarius.io/vsociety/posts/cve-2025-60710-detection-script-eop-vulnerability/">www.vicarius.io/vsociety/posts/cve-2025-60710-detection-script-eop-vulnerability/</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.vicarius.io/vsociety/posts/cve-2025-60710-detection-script-eop-vulnerability/">www.vicarius.io</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>

NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

#### Additional Advisory Data

Source	Time	Event
ADP	2026-04-13T00:00:00.000Z	CVE-2025-60710 added to CISA KEV

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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)