



# Windows Sensor Data Service Elevation of Privilege Vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-26161
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 18:16:48 UTC
<b>Updated</b>	2026-04-17 15:10:35 UTC
<b>Description</b>	Untrusted pointer dereference in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.

## 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:** 0.000730000 probability, percentile 0.220770000 (date 2026-04-21)

**Problem Types:** CWE-20 | CWE-822 | CWE-822 CWE-822: Untrusted Pointer Dereference | CWE-20 CWE-20: Improper Input Validation

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

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Microsoft	<a href="#">Windows 10 Version 1809</a>	affected 10.0.17763.0 10.0.17763.8644 custom	32-bit
CNA	Microsoft	<a href="#">Windows 10 Version 21H2</a>	affected 10.0.19044.0 10.0.19044.7184 custom	32-bit
CNA	Microsoft	<a href="#">Windows 10 Version 22H2</a>	affected 10.0.19045.0 10.0.19045.7184 custom	32-bit
CNA	Microsoft	<a href="#">Windows 11 Version 22H3</a>	affected 10.0.22631.0 10.0.22631.6936 custom	ARM64
CNA	Microsoft	<a href="#">Windows 11 Version 23H2</a>	affected 10.0.22631.0 10.0.22631.6936 custom	x64-bit
CNA	Microsoft	<a href="#">Windows 11 Version 24H2</a>	affected 10.0.26100.0 10.0.26100.8246 custom	ARM64
CNA	Microsoft	<a href="#">Windows 11 Version 25H2</a>	affected 10.0.26200.0 10.0.26200.8246 custom	ARM64
CNA	Microsoft	<a href="#">Windows 11 Version 26H1</a>	affected 10.0.28000.0 10.0.28000.1836 custom	ARM64
CNA	Microsoft	<a href="#">Windows Server 2019</a>	affected 10.0.17763.0 10.0.17763.8644 custom	x64-bit
CNA	Microsoft	<a href="#">Windows Server 2019 Server Core Installation</a>	affected 10.0.17763.0 10.0.17763.8644 custom	x64-bit
CNA	Microsoft	<a href="#">Windows Server 2022</a>	affected 10.0.20348.0 10.0.20348.5020 custom	x64-bit
CNA	Microsoft	<a href="#">Windows Server 2022 23H2 Edition Server Core Installation</a>	affected 10.0.25398.0 10.0.25398.2274 custom	x64-bit
CNA	Microsoft	<a href="#">Windows Server 2025</a>	affected 10.0.26100.0 10.0.26100.32690 custom	x64-bit
CNA	Microsoft	<a href="#">Windows Server 2025 Server Core Installation</a>	affected 10.0.26100.0 10.0.26100.32690 custom	x64-bit

### References

Reference	Source	Link	Tags
<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26161">msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26161</a>	secure@microsoft.com	<a href="https://msrc.microsoft.com">msrc.microsoft.com</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

No vendor comments have been submitted for this CVE.

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

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)