



Windows Local Security Authority Subsystem Service (LSASS) Denial of Service Vulnerability

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-32071 |
| State | PUBLISHED |
| Assigner | microsoft |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-14 18:17:07 UTC |
| Updated | 2026-04-22 17:09:19 UTC |
| Description | Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker |

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secure@microsoft.com

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

EPSS: 0.001350000 probability, percentile 0.331500000 (date 2026-04-22)

Problem Types: CWE-476 | CWE-476 CWE-476: NULL Pointer Dereference

| Version | Source | Type | Score | Severity | Vector |
|---------|----------------------|-----------|-------|----------|--|
| 3.1 | secure@microsoft.com | Secondary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 3.1 | CNA | CVSS | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-----------|--------------------------|---------|--------|---------|----------|
| Operating System | Microsoft | Windows 10 1607 | All | All | All | All |
| Operating System | Microsoft | Windows 10 1607 | All | All | All | All |
| Operating System | Microsoft | Windows 10 1809 | All | All | All | All |
| Operating System | Microsoft | Windows 10 1809 | All | All | All | All |
| Operating System | Microsoft | Windows 10 21h2 | All | All | All | All |
| Operating System | Microsoft | Windows 10 21h2 | All | All | All | All |
| Operating System | Microsoft | Windows 10 21h2 | All | All | All | All |
| Operating System | Microsoft | Windows 10 22h2 | All | All | All | All |
| Operating System | Microsoft | Windows 10 22h2 | All | All | All | All |
| Operating System | Microsoft | Windows 10 22h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 23h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 23h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 24h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 24h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 25h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 25h2 | All | All | All | All |
| Operating System | Microsoft | Windows 11 26h1 | All | All | All | All |
| Operating System | Microsoft | Windows 11 26h1 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2016 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2019 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2022 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2022 23h2 | All | All | All | All |
| Operating System | Microsoft | Windows Server 2025 | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platform |
|--------|-----------|-------------------------|--|----------|
| CNA | Microsoft | Windows 10 Version 1607 | affected 10.0.14393.0 10.0.14393.9060 custom | 32-bit |
| CNA | Microsoft | Windows 10 Version 1809 | affected 10.0.17763.0 10.0.17763.8644 custom | 32-bit |

| | | | | | | | |
|-----|-----------|---|----------|--------------|------------------|--------|---------|
| CNA | Microsoft | Windows 10 Version 21H2 | affected | 10.0.19044.0 | 10.0.19044.7184 | custom | 32-bit |
| CNA | Microsoft | Windows 10 Version 22H2 | affected | 10.0.19045.0 | 10.0.19045.7184 | custom | 32-bit |
| CNA | Microsoft | Windows 11 Version 22H3 | affected | 10.0.22631.0 | 10.0.22631.6936 | custom | ARM64 |
| CNA | Microsoft | Windows 11 Version 23H2 | affected | 10.0.22631.0 | 10.0.22631.6936 | custom | x64-bit |
| CNA | Microsoft | Windows 11 Version 24H2 | affected | 10.0.26100.0 | 10.0.26100.8246 | custom | ARM64 |
| CNA | Microsoft | Windows 11 Version 25H2 | affected | 10.0.26200.0 | 10.0.26200.8246 | custom | ARM64 |
| CNA | Microsoft | Windows 11 Version 26H1 | affected | 10.0.28000.0 | 10.0.28000.1836 | custom | ARM64 |
| CNA | Microsoft | Windows Server 2016 | affected | 10.0.14393.0 | 10.0.14393.9060 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2016 Server Core Installation | affected | 10.0.14393.0 | 10.0.14393.9060 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2019 | affected | 10.0.17763.0 | 10.0.17763.8644 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2019 Server Core Installation | affected | 10.0.17763.0 | 10.0.17763.8644 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2022 | affected | 10.0.20348.0 | 10.0.20348.5020 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2022 23H2 Edition Server Core Installation | affected | 10.0.25398.0 | 10.0.25398.2274 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2025 | affected | 10.0.26100.0 | 10.0.26100.32690 | custom | x64-bit |
| CNA | Microsoft | Windows Server 2025 Server Core Installation | affected | 10.0.26100.0 | 10.0.26100.32690 | custom | x64-bit |

References

| Reference | Source | Link | Tags |
|---|----------------------|---|---------------------|
| msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32071 | secure@microsoft.com | msrc.microsoft.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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](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](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report