



# SymCrypt SymCryptXmssSign function - Heap overflow via 64->32-bit leaf-count truncation

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

## Summary

<b>CVE</b>	CVE-2026-35199
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 20:16:27 UTC
<b>Updated</b>	2026-04-06 20:16:27 UTC
<b>Description</b>	SymCrypt is the core cryptographic function library currently used by Windows. From 103.5.0 to before 103.11.0, The SymC

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from security-advisories@github.com

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

**Problem Types:** CWE-122 | CWE-122 CWE-122: Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	SymCrypt	affected >= 103.5.0, < 103.11.0	Not specified

### References

Reference	Source	Link	Tags
github.com/microsoft/SymCrypt/security/advisories/GHSA-rvj8-8h6x-hjmg	security-advisories@github.com	<a href="https://github.com">github.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, analy

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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