



# UEFI Secure Boot Security Feature Bypass Vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-32220
<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 18:17:29 UTC
<b>Updated</b>	2026-04-17 19:38:26 UTC
<b>Description</b>	Improper access control in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to bypass a

## Risk And Classification

**Primary CVSS:** v3.1 4.4 MEDIUM from secure@microsoft.com

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

**EPSS:** 0.000560000 probability, percentile 0.175020000 (date 2026-04-21)

**Problem Types:** CWE-284 | CWE-284 CWE-284: Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

### 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 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 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 10.0.26100.8246 custom	ARM64-based Syst
CNA	Microsoft	Windows 11 Version 25H2	affected 10.0.26200.0 10.0.26200.8246 custom	ARM64-based Syst
CNA	Microsoft	Windows 11 Version 26H1	affected 10.0.28000.0 10.0.28000.1836 custom	ARM64-based Syst
CNA	Microsoft	Windows Server 2025	affected 10.0.26100.0 10.0.26100.32690 custom	x64-based Systems
CNA	Microsoft	Windows Server 2025 Server Core Installation	affected 10.0.26100.0 10.0.26100.32690 custom	x64-based Systems

### References

Reference	Source	Link	Tags
<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32220">msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32220</a>	secure@microsoft.com	<a href="https://msrc.microsoft.com">msrc.microsoft.com</a>	Vendor Advisory
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.

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)