



# Windows BitLocker Security Feature Bypass Vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-27913
<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 18:16:58 UTC
<b>Updated</b>	2026-04-23 14:55:32 UTC
<b>Description</b>	Improper input validation in Windows BitLocker allows an unauthorized attacker to bypass a security feature locally.

## Risk And Classification

**Primary CVSS:** v3.1 7.7 HIGH from secure@microsoft.com

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

**EPSS:** 0.000730000 probability, percentile 0.221830000 (date 2026-04-21)

**Problem Types:** CWE-20 | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	<a href="#">Windows Server 2012</a>	-	All	All	All
Operating System	Microsoft	<a href="#">Windows Server 2012</a>	r2	All	All	All
Operating System	Microsoft	<a href="#">Windows Server 2016</a>	All	All	All	All
Operating System	Microsoft	<a href="#">Windows Server 2019</a>	All	All	All	All
Operating System	Microsoft	<a href="#">Windows Server 2022</a>	All	All	All	All
Operating System	Microsoft	<a href="#">Windows Server 2022 23h2</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Microsoft	<a href="#">Windows Server 2012</a>	affected 6.2.9200.0 6.2.9200.26026 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2012 Server Core Installation</a>	affected 6.2.9200.0 6.2.9200.26026 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2012 R2</a>	affected 6.3.9600.0 6.3.9600.23132 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2012 R2 Server Core Installation</a>	affected 6.3.9600.0 6.3.9600.23132 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2016</a>	affected 10.0.14393.0 10.0.14393.9060 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2016 Server Core Installation</a>	affected 10.0.14393.0 10.0.14393.9060 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2019</a>	affected 10.0.17763.0 10.0.17763.8644 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2019 Server Core Installation</a>	affected 10.0.17763.0 10.0.17763.8644 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2022</a>	affected 10.0.20348.0 10.0.20348.5020 custom	x64-ba
CNA	Microsoft	<a href="#">Windows Server 2022 23H2 Edition Server Core Installation</a>	affected 10.0.25398.0 10.0.25398.2274 custom	x64-ba

### References

Reference	Source	Link	Tags
<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-27913">msrc.microsoft.com/update-guide/vulnerability/CVE-2026-27913</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.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

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