An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606160509

NCSC Advisory

Security Feature bypass in Windows OS(Multiple) - YellowKey - CVE-2026-45585

17th, June 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-45585

Published: 2026-05-19

Vendor: Microsoft

Product: Windows 11 version 26H1, Windows Server 2025, Windows Server 2025 (Server Core installation), Windows 11 Version 25H2, Windows 11 Version 24H2

CVSS Score[1]: 6.8

Products Affected

Product	Version
Windows 11 Version 24H2	10.0.26100.0 < 10.0.26100.8655
Windows 11 Version 25H2	10.0.26200.0 < 10.0.26200.8655
Windows 11 version 26H1	10.0.28000.0 < 10.0.28000.2269
Windows Server 2025	10.0.26100.0 < 10.0.26100.32995
Windows Server 2025 (Server Core installation)	10.0.26100.0 < 10.0.26100.32995

Impact

CVE-2026-45585 ("YellowKey") is a Windows/BitLocker security feature bypass vulnerability affecting some versions of WinRE. Current information indicates that exploitation requires physical access to the device and primarily targets systems relying on BitLocker protection without additional pre-boot authentication. Microsoft has published mitigations and patches are available.

Systems are at higher risk when:

- BitLocker is enabled using TPM-only protection.
- Devices are frequently taken off-premises (laptops, executive devices, field devices).
- Attackers could gain temporary physical access, such as device located in publically accessible spaces.
- Sensitive data resides on Windows 11 (24H2/25H2/26H1) or Windows Server 2025 systems.

[1] https://www.first.org/cvss/

Mitigations

If you are utilising preboot authentication (TPM + PIN), then this configuration mitigates this vulnerability.

Microsoft have provide a script which they say will mitigate against the vulnerbaility. The script is available on their advisory page at the following url.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585

The other option is to enable TPM + PIN on your devices, this is a more involved and longer strategy but it may make sense from a cyber security standpoint.

Common Weakness Enumeration (CWE)[2]: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Microsoft.

- https://nvd.nist.gov/vuln/detail/CVE-2026-45585
- https://www.cve.org/CVERecord?id=CVE-2026-45585
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog