INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-20 13:51 UTC

YellowKey Zero-Day Bypasses BitLocker Without Credentials, Public PoC Forces Manual Mitigation Across Windows 11 and Server 2025

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0199
Type	CVE Vulnerability
CVE ID	CVE-2026-45585
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0008 (24th percentile)
Affected Products	Windows 11 (24H2, 25H2, 26H1 x64), Windows Server 2025, Windows Server 2025 Server Core
Published	2026-05-20T04:28:26
Discovery Source	Rss

Executive Summary

A publicly disclosed zero-day vulnerability, CVE-2026-45585, allows an attacker with brief physical access and a USB drive to bypass BitLocker encryption on Windows 11 (versions 24H2 through 26H1) and Windows Server 2025, reading protected data without credentials or network access. Microsoft has not issued an automated patch; remediation requires manual intervention on every affected device individually. With a working proof-of-concept publicly available, any unattended or physically accessible endpoint running these operating systems is at immediate risk of unauthorized data access.

Technical Analysis

CVE-2026-45585 (CVSS 7.5, High) is a BitLocker security feature bypass affecting Windows 11 x64 (24H2, 25H2, 26H1) and Windows Server 2025, including Server Core. The attack requires physical access and a USB device; no credentials, software installation, or network connectivity are needed. The attacker boots into or manipulates the Windows Recovery Environment (WinRE) to reach an alternate code path that circumvents BitLocker's authentication gate. Classified under CWE-288 (Authentication Bypass Using an Alternate Path), CWE-693 (Protection Mechanism Failure), and CWE-863 (Incorrect Authorization). MITRE ATT&CK techniques mapped: T1542.001 (Pre-OS Boot: Bootkit), T1200 (Hardware Additions), T1052.001 (Exfiltration over Physical Medium: USB), T1006 (Direct Volume Access). A public PoC exists, materially lowering exploitation difficulty.

Microsoft's response is a mitigation, not a full patch: each affected device requires manual modification of the WinRE image and a TPM configuration change, no automated deployment path is available. EPSS score is 0.00083 (24th percentile), but the existence of a public PoC and the manual-only remediation path elevate practical risk significantly above the EPSS baseline. CVSS vector pending verification from NVD. Note: This CVE is dated 2026 and falls outside training data; all technical details are sourced exclusively from provided advisory material and require validation against Microsoft MSRC advisory before operational use.

Action Checklist

1. Containment: Immediately inventory all Windows 11 (24H2, 25H2, 26H1 x64) and Windows Server 2025 systems (including Server Core) using CIS 1.1 asset inventory. Prioritize devices that are physically accessible to non-authorized personnel: shared workspaces, conference rooms, remote offices, data center colocation, and field-deployed servers. Physically restrict or secure unattended high-risk endpoints pending remediation. Review Microsoft's official MSRC advisory for CVE-2026-45585 to obtain the exact WinRE modification and TPM configuration change procedures (verify the MSRC URL from sources before implementing).
2. Detection: Query your endpoint management platform (SCCM, Intune, or equivalent) for all systems matching the affected OS versions. Enable and review event logs for WinRE boot activity and BitLocker management events (verify event IDs against Microsoft's official Event Viewer documentation for your OS versions). Monitor physical access control logs for after-hours or unauthorized access to device storage areas. Per NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review), establish alerting on anomalous boot sequences. No network-based IOCs are available for this attack vector; detection is endpoint- and physical-access-log-dependent.
3. Eradication: Apply Microsoft's published mitigation for CVE-2026-45585 on every affected device: manually update the WinRE image and apply the required TPM configuration change per the Microsoft MSRC advisory. There is no automated patch path; each device requires hands-on remediation per Microsoft guidance. Track completion per device using your asset inventory (CIS 1.1). Enforce CIS 7.3 (Automated OS Patch Management) posture reviews after the patch becomes available to prevent recurrence. Per NIST SI-2 (Flaw Remediation), document remediation status and test each device after the WinRE update is applied.
4. Recovery: After applying the mitigation on each device, verify BitLocker status and confirm WinRE is updated using Windows system recovery tools per Microsoft documentation. Re-enable any BitLocker protectors that were suspended during the update process. Confirm TPM configuration changes are persistent and not reverted on next boot. Per NIST IR-4 (Incident Handling) and NIST AU-6, review audit logs for any evidence of exploitation prior to remediation. Log remediation completion date and configuration state per device.
5. Post-Incident: Conduct a lessons-learned review against NIST IR-8 (Incident Response Plan) to assess whether your physical access controls and device management procedures were sufficient. Evaluate gaps in: (1) physical security for endpoints handling sensitive data, CIS 3.6 (Encrypt Data on End-User Devices) and the broader physical safeguard posture; (2) WinRE and pre-boot environment change management processes; (3) the ability to deploy emergency manual remediations at scale across the enterprise. Update the remediation process under CIS 7.2 to include manual-only mitigation scenarios. Consider whether BitLocker PIN or network unlock configurations should be enforced as a defense-in-depth measure against pre-boot bypass attacks, consistent with NIST SI-7 (Software, Firmware, and Information Integrity).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if any device shows Event ID 24620 (BitLocker suspension) or 24579 (TPM-only unlock) outside IT-initiated windows during the PoC-public exploitation window, or if any device storing PII, PHI, PCI-in-scope data, or classified information was physically unattended in a shared or public space after the CVE-2026-45585 public PoC release date — regulatory breach notification timelines may be triggered.
Recovery Notes	After applying the WinRE update and TPM configuration change on each device, verify persistence through a full cold-boot cycle (not a warm restart) before marking the device remediated, as some firmware-level TPM changes only commit on a full power cycle. Monitor the Microsoft-Windows-BitLocker-API/Management event log on all remediated devices for 30 days post-remediation for any recurrence of Event ID 24620 or unexpected TPM state changes, which could indicate a failed mitigation or a secondary exploitation attempt. Any device that cannot receive the manual WinRE mitigation within 72 hours should be physically secured (locked cabinet, cable lock, or powered down and stored) until remediation is possible, and must not be left unattended in any shared physical space.
Forensic Artifacts	Microsoft-Windows-BitLocker-API/Management event log (%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-BitLocker-API%4Management.evtx) — CVE-2026-45585 exploitation via WinRE USB boot would produce Event ID 24620 (BitLocker suspension) and/or Event ID 24579 (volume unlocked via TPM without PIN) at the time of physical access, with no corresponding IT change ticket. | Microsoft-Windows-Recovery-Environment/Operational event log (%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Recovery-Environment%4Operational.evtx) — Event ID 1 entries indicate WinRE was invoked; any such entry not correlated with a documented IT maintenance event is a direct IOC for CVE-2026-45585 exploitation. | WinRE image SHA-256 hash of C:\Windows\System32\Recovery\Winre.wim — compare against Microsoft's published hash for the specific OS build; a mismatch indicates the attacker may have modified the WinRE image in addition to reading protected data, indicating a more sophisticated persistent access attempt. | Windows System event log entries for Event ID 12 (OS boot) and Event ID 13 (OS shutdown) — reconstruct unexpected reboot sequences; a reboot sequence with no corresponding user login in the Security log (Event ID 4624) immediately after boot is consistent with a USB-boot WinRE attack that bypassed the normal OS load. | Physical access control system logs (badge reader, CCTV, colocation cage access logs) for the specific device locations — the only way to correlate a WinRE boot event with a specific individual for CVE-2026-45585, given that this attack leaves no network artifacts, no authentication logs in Active Directory, and no remote access traces.

Per-Action IR Details

Containment — Immediately inventory all Windows 11 (24H2, 25H2, 26H1 x64) and Windows Server 2025 systems (including Server Core) using CIS 1.1 asset inventory. Prioritize devices that are physically accessible to non-authorized personnel: shared workspaces, conference rooms, remote offices, data center colocation, and field-deployed servers. Physically restrict or secure unattended high-risk endpoints pending remediation. Review Microsoft's official advisory for CVE-2026-45585 to obtain the exact WinRE modification and TPM configuration change procedures (validate the advisory URL from the source list before citing).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run the following PowerShell one-liner from a management host to enumerate all domain-joined Windows 11 24H2/25H2/26H1 and Server 2025 systems: `Get-ADComputer -Filter * -Properties OperatingSystem,OperatingSystemVersion | Where-Object {$_.OperatingSystem -match 'Windows 11|Windows Server 2025'} | Select-Object Name,OperatingSystem,OperatingSystemVersion | Export-Csv affected_assets.csv -NoTypeInformation`. For non-domain environments, use `nmap -p 445 --script smb-os-discovery ` to fingerprint OS versions. Physically label or cable-lock high-risk endpoints (conference rooms, colocation racks) until the WinRE mitigation is applied. For Server Core systems without a console, verify physical rack access controls and door logs immediately.

Evidence: Before restricting physical access, photograph or document the physical state of each high-risk device (USB ports, attached peripherals, BIOS sticker absence indicating tamper). Check Windows Event Log on each device for Event ID 4608 (Windows Security auditing started) and Event ID 6400–6500 range (BitLocker operational) to establish a pre-incident baseline. Capture `manage-bde -status` output and `reagentc /info` output from every affected device before any remediation — these establish the BitLocker protector state and WinRE status at time of discovery, which is critical if exploitation occurred prior to your response.

Detection — Query your endpoint management platform (SCCM, Intune, or equivalent) for all systems matching the affected OS versions. Enable and review event logs for WinRE boot activity: check Windows Event Log for unexpected entries in the Recovery Environment (EventID 1 in Microsoft-Windows-Recovery-Environment operational log where available) and BitLocker management events (Event IDs 24577–24621 in the Microsoft-Windows-BitLocker-API/Management log). Monitor physical access control logs for after-hours or unauthorized access to device storage areas. Per NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review), establish alerting on anomalous boot sequences. No network-based IOCs are available for this attack vector — detection is endpoint- and physical-access-log-dependent.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without SCCM/Intune, use the PowerShell command `Get-WinEvent -LogName 'Microsoft-Windows-BitLocker-API/Management' -MaxEvents 500 | Where-Object {$_.Id -ge 24577 -and $_.Id -le 24621} | Format-List TimeCreated,Id,Message` on each affected host to pull BitLocker suspension and recovery key access events. For WinRE boot detection, run `Get-WinEvent -LogName 'Microsoft-Windows-Recovery-Environment/Operational' | Format-List` — any Event ID 1 entries not correlated with an IT-initiated maintenance window are suspicious for CVE-2026-45585 exploitation. Deploy a Sigma rule targeting process creation of `reagentc.exe` with arguments `/boottore` or `/enable` outside of your change window using Sysmon Event ID 1. Physical access: cross-reference badge reader or CCTV logs for the specific device locations flagged in containment.

Evidence: The primary forensic signal for CVE-2026-45585 exploitation is a WinRE boot event — capture the full Microsoft-Windows-Recovery-Environment/Operational log (path: `%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Recovery-Environment%4Operational.evtx`) before any remediation wipes it. Collect the Microsoft-Windows-BitLocker-API/Management log (`%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-BitLocker-API%4Management.evtx`) and look specifically for Event ID 24620 (BitLocker suspended by user) or Event ID 24579 (BitLocker volume unlocked without PIN — TPM-only) at timestamps outside IT-initiated windows. Also collect the System event log for Event ID 12 (OS start) and Event ID 13 (OS shutdown) to reconstruct unexpected reboot sequences consistent with a USB-boot attack.

Eradication — Apply Microsoft's published mitigation for CVE-2026-45585 on every affected device: manually update the WinRE image and apply the required TPM configuration change per the Microsoft advisory. There

is no automated patch path — each device requires hands-on remediation. Track completion per device using your asset inventory (CIS 1.1). Enforce CIS 7.3 (Automated OS Patch Management) posture reviews after the patch becomes available to prevent recurrence. Per NIST SI-2 (Flaw Remediation), document remediation status and test each device after the WinRE update is applied.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For a 2-person team managing manual remediation at scale, create a per-device remediation tracking sheet (hostname, OS version, WinRE version pre/post, TPM config state, technician initials, timestamp) and script the pre/post verification steps: pre-patch: `reagentc /info > C:\IR\winre_pre.txt && manage-bde -status >> C:\IR\winre_pre.txt`; post-patch: `reagentc /info > C:\IR\winre_post.txt && manage-bde -status >> C:\IR\winre_post.txt`. Distribute remediation via a USB drive containing the WinRE update script and have each on-site contact run it with local admin credentials, reporting completion via a shared tracking spreadsheet. Prioritize devices in the physical access risk tiers identified during containment — colocation and shared spaces first.

Evidence: Before executing the WinRE update on any device, capture the current WinRE image hash: `Get-FileHash C:\Windows\System32\Recovery\Winre.wim -Algorithm SHA256 | Out-File C:\IR\winre_hash_pre.txt`. This provides a forensic baseline to confirm the WinRE image was not already tampered with by an attacker leveraging CVE-2026-45585 to implant a backdoored recovery image. Also export the current TPM status via `Get-Tpm | Export-Clixml C:\IR\tpm_state_pre.xml` before applying the TPM configuration change. If the WinRE image hash does not match Microsoft's published hash for the current OS build, treat the device as potentially compromised and escalate before proceeding with eradication.

Recovery — After applying the mitigation on each device, verify BitLocker status using 'manage-bde -status' and confirm WinRE is updated ('reagentc /info'). Re-enable any BitLocker protectors that were suspended during the update process. Confirm TPM configuration changes are persistent and not reverted on next boot. Per NIST IR-4 (Incident Handling) and NIST AU-6, review audit logs for any evidence of exploitation prior to remediation — specifically, look for unexpected WinRE boot events or BitLocker suspension events not initiated by IT staff. Log remediation completion date and configuration state per device.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Post-remediation verification script for each device (run as administrator): `manage-bde -status C: | Select-String 'Protection Status','Key Protectors','Conversion Status'` — confirm 'Protection Status: Protection On' and that TPM is listed as a key protector. Then run `reagentc /info` and confirm 'Windows RE status: Enabled' and that the WinRE image path reflects the updated image. Force a cold reboot (not restart) and re-run both checks to confirm TPM configuration changes survive a full power cycle, since some firmware-level changes only persist after a full shutdown cycle. For Server Core systems, run these same commands remotely via `Invoke-Command -ComputerName -ScriptBlock {manage-bde -status C:; reagentc /info}` from a management host.

Evidence: During recovery verification, collect the post-remediation BitLocker-API/Management event log and diff it against the pre-remediation snapshot to identify any Event ID 24620 (suspension) or Event ID 24579 (TPM-only unlock) events that occurred in the window between public PoC release and your containment action — this is your exploitation window. Export `Get-Tpm` output post-reboot to `C:\IR\tpm_state_post.xml` and compare against the pre-remediation XML to confirm the TPM configuration change is persistent. Retain both pre- and post-remediation WinRE image hashes and the full event log exports as incident evidence per NIST AU-11 (Audit Record Retention).

Post-Incident — Conduct a lessons-learned review against NIST IR-8 (Incident Response Plan) to assess whether your physical access controls and device management procedures were sufficient. Evaluate gaps in: (1) physical security for endpoints handling sensitive data — CIS 3.6 (Encrypt Data on End-User Devices) and the broader physical safeguard posture; (2) WinRE and pre-boot environment change management processes; (3) the ability to deploy emergency manual remediations at scale across the enterprise. Update the remediation process under CIS 7.2 to include manual-only mitigation scenarios. Consider whether BitLocker PIN or network unlock configurations should be enforced as a defense-in-depth measure against pre-boot bypass attacks, consistent with NIST SI-7 (Software, Firmware, and Information Integrity).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 3.6 (Encrypt Data on End-User Devices), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Document the lessons-learned output in a structured format tied directly to CVE-2026-45585 gaps: (1) time-to-inventory for affected OS versions, (2) time-to-physical-containment for high-risk locations, (3) manual remediation throughput (devices/day per technician). Use this data to calculate the exploitation window exposure duration. For BitLocker PIN enforcement as a compensating control against future pre-boot bypass attacks, use Group Policy (GPO path: `Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication at startup`) to enforce TPM+PIN on all laptops and field-deployed systems — this requires no additional tooling and eliminates the TPM-only unlock path that CVE-2026-45585 exploits. Document this GPO change in your change management system as a direct output of the post-incident review.

Evidence: Compile the complete incident artifact package for retention: all pre/post `manage-bde -status` outputs, WinRE image hashes, TPM state XML exports, BitLocker-API/Management event log archives, the affected asset inventory CSV, physical access log excerpts for the exploitation window, and the per-device remediation tracking sheet. Retain per NIST AU-11 (Audit Record Retention) and your organization's records retention policy. If any device showed Event ID 24620 or 24579 outside IT-initiated windows during the exploitation window, those devices should be treated as potentially compromised and escalated for full forensic review before being returned to production — do not close the incident for those specific assets until a forensic examination rules out data exfiltration via the BitLocker bypass.

Detection Guidance

This attack vector is entirely physical and offline; no network-based IOC detection applies. Detection depends on endpoint telemetry and physical access logging. (1) OS version exposure: Query endpoint management tools (Intune, SCCM, or equivalent) for all assets running Windows 11 24H2, 25H2, 26H1 x64 or Windows Server 2025. Cross-reference against your CIS 1.1 asset inventory. (2) WinRE boot events: Monitor recovery environment operational logs for unexpected boot-into-recovery events, particularly outside of IT maintenance windows. Verify specific event IDs against Microsoft's official Event Viewer documentation for your OS versions. Correlate with physical access control logs. (3) BitLocker event log: Query BitLocker management logs for suspension or protector-removal events not initiated by authorized IT processes. (4) TPM state changes: Use platform-specific tooling to audit TPM configuration state across the fleet; unexpected TPM changes warrant investigation. (5) Physical access anomalies: Cross-reference data center or office badge-access logs against known IT staff activity windows. No file hashes, IPs, domains, or network signatures are available for this vulnerability. Per NIST AU-2 (Event Logging), ensure pre-boot and recovery environment events are captured where logging capability exists.

Framework Mappings

MITRE-ATTACK

- **T1542.001** — System Firmware
- **T1200** — Hardware Additions
- **T1052.001** — Exfiltration over USB
- **T1006** — Direct Volume Access

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

NIST-800-53R5

- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.8** — Define and Maintain Role-Based Access Control
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1542.001	System Firmware	Persistence

Technique ID	Technique Name	Tactic
T1200	Hardware Additions	Initial-Access
T1052.001	Exfiltration over USB	Exfiltration
T1006	Direct Volume Access	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/microsoft-releases-mitigation-for...	T3
CVE-2026-45585 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-45585	T1
Microsoft is aware of a security feature bypass... · CVE-2026-45585	https://github.com/advisories/GHSA-2h24-8rjh-qgjv	T3
CVE-2026-45585: CWE-77: Improper Neutralization of Special ...	https://radar.offseq.com/threat/cve-2026-45585-cwe-77-improper-neut...	T3
Common Vulnerabilities and Exposures (CVEs) | Tenable®	https://www.tenable.com/cve	T3

Generated 2026-05-20 13:51 UTC by TJS Security Command Center