INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:12 UTC

April 2026 Windows 11 Update KB5083769 Breaks VSS, Disabling Backup Pipelines Across Multiple Vendors

SECURITY ANALYSIS | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-STY-2026-0101
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Windows 11 24H2, Windows 11 25H2; Acronis Cyber Protect Cloud, Macrium Reflect, NinjaOne Backup, UrBackup Server
Published	2026-04-30T11:23:03
Discovery Source	Rss

Executive Summary

Microsoft's April 2026 cumulative update KB5083769 has introduced a defect in the Windows Volume Shadow Copy Service (VSS) that breaks snapshot creation on Windows 11 24H2 and 25H2, silently disabling backup pipelines across multiple enterprise backup platforms including Acronis, Macrium Reflect, NinjaOne, and UrBackup. The failure is not a cyberattack, but its operational consequence is identical to one: affected organizations lose the ability to create reliable recovery points, eliminating a primary ransomware mitigation control until the update is uninstalled. Microsoft has not released a fix; the only confirmed remediation is rolling back the patch, forcing security teams to choose between patch currency and backup continuity.

Technical Analysis

KB5083769, Microsoft's April 2026 cumulative update for Windows 11 24H2 and 25H2, introduces a regression in VSS that causes snapshot creation requests to time out rather than complete. VSS is the foundational Windows subsystem that backup products use to capture application-consistent point-in-time snapshots of live volumes. When VSS fails, any backup product that depends on it fails silently or with errors, the backup job appears to run but produces no usable recovery point.

Affected products confirmed at time of reporting include Acronis Cyber Protect Cloud, Macrium Reflect, NinjaOne Backup, and UrBackup Server. The Acronis impact is compounded: the defect also severs connectivity between affected endpoints and the Acronis cloud management console, causing endpoints to

appear offline. This means administrators may not immediately recognize that backups have failed, they may see connectivity errors and misattribute them to network or agent issues rather than the underlying VSS regression.

This is a quality regression tagged under CWE-400 (uncontrolled resource consumption), consistent with the VSS timeout behavior described. No CVE ID has been assigned, which aligns with this being a product defect rather than a disclosed vulnerability. The defect has not received an official CVSS score from NVD or MSRC.

The strategic consequence is significant. Organizations running these backup products on affected Windows 11 builds currently have no valid recovery point generation. The practical exposure window is the interval between the April patch deployment and either Microsoft's release of a corrected update or the organization's rollback of KB5083769. Patch management teams that auto-deploy monthly updates may have already propagated the defect widely before backup failures were detected. Source: BleepingComputer (https://www.bleepingcomputer.com/news/microsoft/april-kb5083769-windows-11-update-causes-backup-software-failures/), April 2026.

Action Checklist

1. Step 1: Assess exposure, identify all Windows 11 24H2 and 25H2 endpoints in your environment and confirm whether KB5083769 has been deployed via Windows Update history, WSUS, or your patch management console
2. Step 2: Validate backup state, run a test VSS snapshot manually (vssadmin create shadow /for=C:) on affected endpoints; a successful snapshot should complete without timeout errors. Verify that Acronis, Macrium, NinjaOne, or UrBackup jobs are producing valid recovery points, not silent failures or incomplete jobs
3. Step 3: Decide on rollback, if VSS failures are confirmed, evaluate uninstalling KB5083769 as the only confirmed workaround; weigh this against the security posture impact of running without April 2026 security fixes and document the decision for your risk register
4. Step 4: Check Acronis console for ghost endpoints, if running Acronis Cyber Protect Cloud, audit the management console for endpoints showing as offline that were previously connected; do not assume offline status reflects network or agent issues without ruling out the KB5083769 defect first
5. Step 5: Monitor for Microsoft guidance, track Microsoft's Known Issues page for KB5083769, the Microsoft Release Health dashboard, and vendor advisories from Acronis, Macrium, NinjaOne, and UrBackup for updated workarounds or a corrected cumulative update; do not re-deploy KB5083769 until vendor compatibility is confirmed

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO or IT leadership immediately if any affected endpoint is a system that stores regulated data (PII, PHI, PCI-DSS cardholder data) where backup failure triggers a gap in data availability controls required by HIPAA §164.308(a)(7), PCI DSS Requirement 12.3, or applicable data retention regulations, or if more than 20% of Windows 11 24H2/25H2 endpoints are confirmed to have had no successful backup since KB5083769 deployment, indicating a material business continuity risk.

Recovery Notes	After rollback of KB5083769, run `vssadmin create shadow /for=C:` on a representative sample of previously affected endpoints and confirm successful shadow copy creation before re-enabling automated backup jobs in Acronis, Macrium, NinjaOne, or UrBackup — do not assume the uninstall restored VSS until a successful manual snapshot is verified. Once automated backup jobs resume, validate that the first three consecutive scheduled backup jobs for each affected endpoint produce recovery points flagged as Successful (not just Completed with warnings) in the respective backup console. Monitor Windows Application Event Log VSS source events (IDs 8193, 8194, 12289, 12293) daily for the first two weeks post-rollback to catch any VSS regression before it silently propagates into another missed backup window, and re-evaluate re-deployment of KB5083769 only after Microsoft publishes a superseding cumulative update with explicit VSS compatibility confirmation from all four affected backup vendors.
Forensic Artifacts	Windows Application Event Log — VSS source entries (Event IDs 8193, 8194, 12289, 12293) timestamped after KB5083769 installation: these record VSS writer failures and provider errors that directly evidence the backup pipeline breakage caused by this specific update defect | vssadmin list writers output captured post-KB5083769 installation: writers showing State [13] Failed or Last Error: Non-retryable error confirm the VSS subsystem degradation specific to this defect and distinguish it from normal transient VSS writer timeouts | Acronis Cyber Protect Cloud agent logs at C:\ProgramData\Acronis\BackupClient\Logs\ — entries timestamped after KB5083769 installation showing VSS snapshot initiation failures, providing vendor-specific evidence that the Acronis backup pipeline was broken by the update rather than by an agent or network issue | Windows Update log (exported via Get-WindowsUpdateLog to WindowsUpdate.log) and C:\Windows\SoftwareDistribution\ReportingEvents.log — these establish the precise KB5083769 installation timestamp, enabling correlation with the first backup job failures in Macrium Reflect (C:\ProgramData\Macrium\Reflect\Logs\) or UrBackup server job history logs to confirm causation | Backup job history exports from the management consoles of Acronis Cyber Protect Cloud, NinjaOne, Macrium Reflect, and UrBackup showing job status transitions from Successful to Failed or Silent Failure aligned with KB5083769 deployment date — this cross-vendor artifact set documents the blast radius and supports the risk register entry justifying rollback

Per-Action IR Details

Step 1: Assess exposure — identify all Windows 11 24H2 and 25H2 endpoints in your environment and confirm whether KB5083769 has been deployed via Windows Update history, WSUS, or your patch management console

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: scope identification and asset enumeration to bound the incident

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run the following PowerShell one-liner across reachable endpoints using WinRM or as a scheduled task deployed via GPO: `Get-HotFix -Id KB5083769 | Select-Object PSComputerName, InstalledOn`. For environments without WinRM, query WSUS approval and deployment status via the WSUS console under Reports > Update Detailed Status filtered on KB5083769. If neither is available, parse C:\Windows\Logs\CBS\CBS.log on each host for the string 'KB5083769' to confirm installation.

Evidence: Before enumerating, capture a point-in-time snapshot of the WSUS or patch console deployment report for KB5083769 showing per-endpoint install status and timestamps. On individual endpoints, preserve: (1) output of

`Get-HotFix` showing KB5083769 InstalledOn date, (2) contents of C:\Windows\SoftwareDistribution\ReportingEvents.log showing the update installation event, and (3) Windows Update logs exportable via `Get-WindowsUpdateLog` (outputs to %USERPROFILE%\Desktop\WindowsUpdate.log) — these establish the exact deployment timeline needed to correlate backup job failures to the update installation date.

Step 2: Validate backup state — run a test VSS snapshot manually (vssadmin create shadow) on affected endpoints to confirm whether VSS is functional; also verify that Acronis, Macrium Reflect, NinjaOne, or UrBackup jobs are producing valid recovery points, not silent failures

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: validating scope and confirming impact through direct technical testing

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Run `vssadmin create shadow /for=C:` from an elevated command prompt and capture the full output — success returns a shadow copy ID, failure returns VSS error codes (0x80042306 or 0x80042302 are characteristic of VSS writer registration failures post-KB5083769). Additionally run `vssadmin list writers` and look for any writer showing State: [13] Failed or Last Error: Non-retryable error. For Macrium Reflect, check the Macrium log at C:\ProgramData\Macrium\Reflect\Logs\ for 'VSS Error' entries timestamped after KB5083769 installation. For UrBackup, query the server web UI job history or parse UrBackup server logs at the configured log directory for 'shadow copy creation failed' strings. For NinjaOne, check the NinjaRMM agent log at C:\ProgramData\NinjaRMMAgent\ninjarmm-agent.log for backup job exit codes.

Evidence: Capture before testing: (1) output of `vssadmin list shadowstorage` and `vssadmin list shadows` to document any existing shadow copies and their creation timestamps — establish whether the last successful shadow predates KB5083769 installation; (2) Windows Application Event Log entries from source 'VSS' (Event IDs 8193, 8194, 12289, 12293) which record VSS writer and provider failures — export with `wevtutil qe Application /q:"*[System[Provider[@Name='VSS']]]" /f:text > vss_errors.txt`; (3) Acronis agent logs at C:\ProgramData\Acronis\BackupClient\Logs\ showing job completion status and VSS interaction errors prior to your test run.

Step 3: Decide on rollback — if VSS failures are confirmed, evaluate uninstalling KB5083769 as the only confirmed workaround; weigh this against the security posture impact of running without April 2026 security fixes and document the decision for your risk register

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: selecting containment strategy that balances operational continuity against security risk, with explicit risk acceptance documentation

Controls: NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), NIST CM-4 (Impact Analyses), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: To uninstall KB5083769 without SCCM/Intune, run from an elevated prompt: `wusa /uninstall /kb:5083769 /quiet /norestart` then schedule a maintenance window reboot. Confirm removal with `Get-HotFix -Id KB5083769` returning no results. Document the rollback decision in a risk register entry that records: date of decision, confirmed VSS failure evidence, specific April 2026 CVEs patched by KB5083769 that now lack coverage (retrieve from the Microsoft Security Update Guide filtered on KB5083769), compensating controls applied, and the name/role of the approver. Apply compensating controls for unpatched exposure: enable Windows Defender Attack Surface Reduction rules via `Set-MpPreference` and confirm Windows Firewall inbound rules are at their most restrictive posture.

Evidence: Before executing rollback, preserve a full forensic record of the failed backup state: (1) export Windows Application and System Event Logs in EVTX format (`wevtutil epl Application Application_pre_rollback.evtx` and same for System log) to establish a pre-rollback baseline; (2) run `vssadmin list writers > vss_writers_pre_rollback.txt` and `vssadmin list providers > vss_providers_pre_rollback.txt` to document the degraded VSS state before the uninstall

modifies it; (3) record installed update list via `Get-HotFix | Export-Csv hotfixes_pre_rollback.csv` — this becomes your evidence of the security delta between patched and rolled-back states for the risk register.

Step 4: Check Acronis console for ghost endpoints — if running Acronis Cyber Protect Cloud, audit the management console for endpoints showing as offline that were previously connected; do not assume offline status reflects network or agent issues without ruling out the KB5083769 defect first

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlation of indicators across multiple systems to accurately scope impact and avoid misattribution

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: In the Acronis Cyber Protect Cloud management console, navigate to Devices > All Devices and filter by Status = Offline. Export the list. For each offline endpoint, cross-reference against your KB5083769 deployment list from Step 1 — endpoints appearing in both lists are high-confidence KB5083769 casualties rather than genuine connectivity or agent failures. On endpoints you can still reach, check the Acronis agent service state: `Get-Service -Name 'Acronis Managed Machine Service'` — if the service is running but the console shows offline, this is consistent with VSS-induced agent communication failures, not a network outage. Review Acronis agent logs at C:\ProgramData\Acronis\BackupClient\Logs\ for VSS-related error strings immediately following KB5083769 installation timestamp.

Evidence: Capture before auditing the Acronis console: (1) a timestamped export or screenshot of the Acronis Cyber Protect Cloud device list showing offline/online status — this is your pre-investigation baseline and establishes when the offline state first appeared relative to KB5083769 deployment; (2) Windows System Event Log entries for Event ID 7036 (Service Control Manager — service state changes) from the VSS service and Acronis agent service around the time of KB5083769 installation, exportable via `wevtutil qe System /q:"*[System[Provider[@Name='Service Control Manager'] and EventID=7036]]" /f:text > scm_events.txt`; (3) Acronis agent communication logs showing last successful heartbeat timestamp to the cloud console — this timestamp correlated against the KB5083769 installation time confirms causation.

Step 5: Monitor for Microsoft guidance — track Microsoft's Known Issues page for KB5083769, the Microsoft Release Health dashboard, and vendor advisories from Acronis, Macrium, NinjaOne, and UrBackup for updated workarounds or a corrected cumulative update; do not re-deploy KB5083769 until vendor compatibility is confirmed

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned, monitoring for resolution, and updating procedures to prevent recurrence; also maps to NIST 800-61r3 §2 — Preparation (maintaining situational awareness infrastructure)

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Set up free monitoring without a commercial threat intel platform: (1) subscribe to the Microsoft Release Health RSS feed at https://learn.microsoft.com/api/search/rss?search=KB5083769&locale=en-us (validate this URL resolves — treat as a search-retrieved reference requiring human confirmation) or bookmark the Windows 11 known issues page directly; (2) create a free account on the CISA Known Exploited Vulnerabilities feed (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) — if any CVE patched exclusively by KB5083769 appears here, the rollback risk calculus changes immediately; (3) subscribe to vendor advisory mailing lists for Acronis (support.acronis.com), Macrium (macrium.com/support), and UrBackup (urbackup.org) directly; (4) set a calendar reminder for the second Tuesday of May 2026 (next Patch Tuesday) as the earliest realistic date for a corrected cumulative update that would supersede KB5083769.

Evidence: Maintain a living evidence log for this incident: (1) preserve all vendor advisory PDFs or web captures from Acronis, Macrium, NinjaOne, and UrBackup acknowledging the KB5083769 VSS incompatibility — these establish vendor-confirmed scope and support change management justification for the rollback; (2) retain the Microsoft Update Catalog entry for KB5083769 showing its included security fixes, to document the specific CVEs your environment lacks coverage for during the rollback period; (3) after re-deploying a corrected update, run `vssadmin create shadow /for=C:` again and preserve the successful output as evidence of VSS restoration — this closes the incident record with verified remediation.

Detection Guidance

The primary detection signal is VSS failure events in the Windows Event Log. Review the Application log for VSS source errors (Event IDs 8193, 8194, 12293, and 13 are common VSS failure indicators per Windows Event Viewer documentation). Review the System log for timeout-related entries tied to the VSS service.

For Acronis environments specifically: endpoints appearing offline in the cloud console without a corresponding network or agent change should be treated as a VSS-related symptom until ruled out.

For all affected backup products: review backup job logs for failed or incomplete jobs initiated after KB5083769's deployment date. Compare job completion timestamps against patch deployment timestamps, a gap strongly suggests the defect is the cause.

Hunting hypothesis: query your patch management or endpoint management platform for all Windows 11 devices where KB5083769 is installed AND the last successful backup timestamp predates the patch deployment date. That intersection defines your confirmed exposure population.

Policy gap to audit: verify whether your backup monitoring alerts on silent job failures (jobs that complete without error codes but produce no usable snapshot), this incident demonstrates that VSS-dependent backups can fail without generating obvious alerts in some configurations.

Framework Mappings

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **SI-2** — Flaw Remediation
- **SR-2** — Supply Chain Risk Management Plan

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/microsoft/april-kb5083769-win...	T3
	https://www.bleepingcomputer.com/news/microsoft/april-kb5083769-win...	T3
	https://www.bleepingcomputer.com/news/microsoft/microsoft-pulls-win...	T3
	https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-out...	T3
Acronis Products: The latest security patches	https://care.acronis.com/s/article/Acronis-fixed-security-vulnerabi...	T3

Generated 2026-05-01 07:12 UTC by TJS Security Command Center