INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 13:58 UTC

Microsoft Declines to Patch Windows Search URI Handler NTLMv2 Hash Leak (CVE-2026-33829)

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0261
Type	CVE Vulnerability
CVE ID	CVE-2026-33829, CVE-2023-35636
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0026 (50th percentile)
Affected Products	Microsoft Windows, 'search:' / ms-search: URI handler (all supported Windows versions with default SMB authentication behavior)
Published	2026-06-03T06:18:52
Discovery Source	Rss

Executive Summary

Microsoft has formally declined to patch CVE-2026-33829, a vulnerability in the Windows 'search:' URI handler that allows attackers to capture NTLMv2 credential hashes by tricking users into clicking a malicious link. All supported Windows versions are affected, and no vendor-supplied fix is forthcoming, leaving every Windows enterprise environment dependent on compensating controls. The business risk is credential exposure leading to lateral movement, privilege escalation, and potential domain compromise, with no patch timeline to cite to auditors or the board.

Technical Analysis

CVE-2026-33829 affects the Windows 'search:' and 'ms-search:' URI handlers across all supported Windows versions (Windows 10, 11, Server 2016/2019/2022/2025). When a user clicks a crafted URI, Windows triggers an outbound SMB authentication attempt (TCP 445) to an attacker-controlled server, exposing the victim's NTLMv2 hash. The hash can be cracked offline or relayed (Pass-the-Hash, T1550.002) to authenticate against internal resources without knowing the plaintext password. The attack requires no special privileges and minimal user interaction - a single click on a malicious link, including those delivered via targeted phishing email (T1566.002 - Phishing: Email). The vulnerability maps to CWE-294 (Authentication Bypass by Capture-Replay), CWE-522 (Insufficiently Protected Credentials), and potentially CWE-436 (Improper Handling of URI Input Validation). MITRE ATT&CK techniques: T1187 (Forced Authentication), T1557.001 (LLMNR/NBT-NS

Poisoning and SMB Relay), T1550.002 (Pass the Hash), T1021.002 (Remote Service Session Initiation: SMB/Windows Admin Shares for post-compromise lateral movement). Microsoft classified the issue below its servicing threshold and issued no patch. The pattern directly mirrors CVE-2023-35636 (Outlook calendar URI NTLMv2 leak), indicating a structural authentication weakness in Windows URI handler architecture. EPSS score: 0.0026 (49th percentile). CISA KEV: not listed. CVSS base: 7.5 (vendor did not assign official score via MSRC; base score reflects NVD assessment). No patch is available; compensating controls are the only defense. Note: Technical claims are grounded in NIST NVD and vendor advisory sources (T1 authority); security news and community forums provide discovery and discussion context only.

Action Checklist

1. Step 1: Containment, Block outbound SMB (TCP 445 and TCP 139) at all perimeter and internal segmentation firewalls immediately. This prevents NTLMv2 hash capture even if a malicious URI is clicked. Verify the block applies to all egress paths, including cloud-hosted Windows workloads and VPN-connected endpoints. Reference: NIST SC-7 (Boundary Protection), CIS Controls v8.1 4.4 and 4.5.
2. Step 2: Detection, Query firewall and proxy logs for outbound TCP 445 connections from workstations to non-RFC1918 external IPs. In Windows Security event logs, look for Event ID 4648 (logon attempt using explicit credentials) and Event ID 4624 with NTLM logon type (Type 3) to unfamiliar destinations. Correlate event timestamps and source account with network logs to identify accounts authenticating via NTLM to external IPs. In EDR telemetry, hunt for processes spawning SMB authentication to external IPs following URI handler invocation (search: or ms-search: protocol). Reference: NIST AU-6, AU-12, SI-4 (System Monitoring), CIS Controls v8.1 8.2.
3. Step 3: Eradication, No vendor patch exists. Apply the following compensating controls in priority order: (1) Verify Group Policy: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > 'Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Deny all' or 'Deny all except for allowed servers' (Microsoft KB #5005413). (2) Optionally disable the 'search:' and 'ms-search:' URI protocol handlers via registry policy (HKEY_CLASSES_ROOT\search and ms-search) on systems where Windows Search URI functionality is confirmed unused. WARNING: Test on non-production pilot systems first; disabling URI handlers may break Windows Search integration in some applications. Prepare rollback procedure before applying. (3) Enable SMB signing enterprise-wide to mitigate relay attacks via Group Policy: 'Microsoft network server: Digitally sign communications (always)' = Enabled. Reference: NIST IA-3, SC-8, Microsoft KB #5005413.
4. Step 4: Recovery, After controls are applied, validate outbound SMB block with a controlled test from an internal workstation to a monitored external IP on TCP 445 (should be blocked). Confirm Group Policy NTLM and SMB signing settings have propagated via 'gpresult /r' on sample endpoints. Run a targeted hunt for any NTLMv2 authentication events (Event IDs 4624, 4648, logon type 3) in the 30 days prior to control implementation to assess whether exploitation occurred before remediation. Cross-reference with network logs to identify any accounts showing outbound NTLM authentication to external IPs. Reset credentials for any accounts showing anomalous NTLM authentication patterns. Reference: NIST IR-4, AU-6.
5. Step 5: Post-Incident, Document this item as a permanent compensating control gap requiring annual review, since no patch is forthcoming. Add the outbound SMB block and NTLM restriction to your security baseline and CIS Controls benchmark validation (CIS Controls v8.1 4.4, 4.5). Review whether other Windows URI handlers (ms-word:, ms-excel:, ms-powerpoint:, mailto:) require similar audit; the structural weakness identified here applies broadly. Update your NTLM usage inventory and set a target date for

Kerberos-only enforcement in line with NIST IA-8 and AC-17. Reference: NIST PM-6, CA-7, SC-8.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if the 30-day retroactive NTLM hunt (Step 4) identifies any NTLMv2 authentication events from workstation accounts to external IPs — this constitutes evidence of potential credential theft requiring breach notification assessment, particularly if the affected accounts had access to PII, PHI, or PCI-scoped systems.
Recovery Notes	After outbound SMB block and NTLM compensating controls are confirmed propagated, maintain elevated monitoring on domain controller Security event logs for Event ID 4776 (NTLM credential validation) and Event ID 4769 (Kerberos service ticket requests) for anomalous service access patterns for a minimum of 30 days, as captured NTLMv2 hashes may have been cracked offline and used post-remediation. Any privileged account (Domain Admin, service accounts) that authenticated via NTLM to an external destination during the exposure window must be treated as fully compromised — reset credentials, audit all actions taken during the exposure window, and consider golden ticket invalidation (krbtgt password double-reset) if domain admin hashes may have been captured. Retain all log artifacts collected during this incident for a minimum of 12 months given the unpatched permanent nature of CVE-2026-33829.
Forensic Artifacts	Windows Security Event Log (Security.evtx) on domain controllers and workstations: Event ID 4776 (NTLM credential validation — the server-side record of NTLMv2 challenge/response triggered when the search: URI handler directed SMB authentication to an attacker-controlled host) and Event ID 4648 (explicit credential logon attempt) — these are the primary indicators that hash capture occurred. | Sysmon Event ID 3 (Network Connection) logs from workstations: filter for outbound connections on destination port 445 where the initiating process is searchprotocolhost.exe, searchindexer.exe, or explorer.exe — this process-to-network correlation uniquely fingerprints CVE-2026-33829 exploitation versus legitimate SMB traffic. | Windows Registry key HKCU\Software\Microsoft\Windows\Shell\MuiCache and HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist on affected workstations: these persist evidence of search: and ms-search: URI invocations and can establish the timeline of when a malicious link was clicked even after browser history is cleared. | Web proxy or Secure Web Gateway access logs: look for HTTP/HTTPS requests containing 'search:' or 'ms-search:' in the URI or referrer fields — this identifies the malicious web page or phishing email origin that delivered the exploit link, and the timestamp anchors the start of the exploitation window. | Network flow data (NetFlow/IPFIX) or perimeter firewall connection logs: TCP 445 outbound connection records from workstation IPs to non-RFC1918 destination IPs during the exposure window — even after the block is applied, historical flow data from the 30-day lookback is the primary evidence source for determining whether exploitation preceded remediation.

Per-Action IR Details

Step 1: Containment — Block outbound SMB (TCP 445 and TCP 139) at all perimeter and internal segmentation firewalls immediately. This prevents NTLMv2 hash capture even if a malicious URI is clicked. Verify the block applies to all egress paths, including cloud-hosted Windows workloads and VPN-connected endpoints. Reference: NIST SC-7 (Boundary Protection), CIS 4.4, CIS 4.5.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Windows hosts without enterprise firewall management, run: `netsh advfirewall firewall add rule name='Block Outbound SMB 445' dir=out protocol=TCP remoteport=445 action=block` and duplicate for port 139. For VPN-split-tunnel endpoints where perimeter rules do not apply, deploy this via a GPO startup script or push via PSExec to all workstations. Verify enforcement with: `netsh advfirewall firewall show rule name='Block Outbound SMB 445'`. Use Wireshark on a monitored egress point to confirm no TCP 445 SYN packets are leaving the environment post-block.

Evidence: Before blocking, capture a 15-minute packet capture on the perimeter firewall egress interface filtered for `tcp.port == 445 and ip.dst != ` to establish whether any outbound SMB connections to external IPs are already in progress, which would indicate prior exploitation. Preserve firewall flow logs (NetFlow/IPFIX) covering the 30 days prior to block implementation. Export Windows Firewall operational log from `%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx` on key workstations before rule changes overwrite baseline state.

Step 2: Detection — Query firewall and proxy logs for outbound TCP 445 connections from workstations to non-domain external IPs. In Windows Security event logs, look for Event ID 4648 (logon attempt using explicit credentials) and Event ID 4624/4625 with NTLM logon type (Type 3) to unfamiliar destinations. In EDR telemetry, hunt for processes spawning SMB authentication to external IPs following URI handler invocation (search: or ms-search: protocol). Reference: NIST AU-6, AU-12, CIS 8.2.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following PowerShell on each Windows host to extract NTLM authentication events targeting external IPs from the Security event log: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648) -and $_.Message -match 'NtLmSsp'} | Select-Object TimeCreated, Id, Message | Export-Csv ntlm_auth_audit.csv`. For process-level correlation, deploy Sysmon with a config that logs Event ID 3 (Network Connection) filtered on destination port 445 and source process not in `System, lsass.exe` — any `explorer.exe`, `searchprotocolhost.exe`, or browser process initiating TCP 445 to an external IP is a high-fidelity indicator of CVE-2026-33829 exploitation. Cross-reference Sysmon Event ID 1 (Process Create) for `searchprotocolhost.exe` or `searchindexer.exe` launched shortly before the outbound connection.

Evidence: Collect from each suspect workstation: (1) Windows Security Event Log entries for Event IDs 4624, 4625, and 4648 with Logon Type 3 (Network) and Authentication Package 'NTLM' or 'NtLmSsp' — these represent the NTLMv2 challenge/response triggered by the URI handler resolving to an attacker-controlled SMB server. (2) Sysmon Event ID 3 logs showing outbound connections on port 445 from `searchprotocolhost.exe` or `explorer.exe`. (3) Browser history and Windows URI handler invocation logs — check `HKCU\Software\Microsoft\Windows\Shell\MuiCache` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist` for evidence of `search:` or `ms-search:` URI activation. (4) IIS or web proxy access logs showing the referrer URL containing `search:` or `ms-search:` protocol strings, indicating the malicious link origin.

Step 3: Eradication — No vendor patch exists. Apply the following compensating controls in priority order: (1) Disable NTLMv2 authentication where Kerberos can substitute, via Group Policy (Network Security: LAN Manager Authentication Level set to 'Send NTLMv2 response only / refuse LM and NTLM'). (2) Block the 'search:' and 'ms-search:' URI protocol handlers via registry policy (HKEY_CLASSES_ROOT\search and ms-search keys) on systems where Windows Search URI functionality is not required. (3) Enable SMB signing enterprise-wide to mitigate relay attacks even if hash capture occurs. Reference: NIST IA-3, SC-8, D3-CH (Credential Hardening), D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-3 (Device Identification and Authentication), NIST SC-8 (Transmission Confidentiality and Integrity), NIST AC-17 (Remote Access), NIST CM-6 (Configuration Settings), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For teams without GPO infrastructure: (1) Set LAN Manager Authentication Level via registry: `reg add 'HKLM\SYSTEM\CurrentControlSet\Control\Lsa' /v LmCompatibilityLevel /t REG_DWORD /d 5 /f` (value 5 = refuse LM and NTLM, accept NTLMv2 only; note this does NOT prevent hash capture via CVE-2026-33829 but limits downgrade attacks). (2) Disable the search: URI handler: `reg delete 'HKCR\search' /f` and `reg delete 'HKCR\ms-search' /f` — back up the keys first with `reg export HKCR\search search_backup.reg`. (3) Enable SMB signing: `reg add 'HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters' /v RequireSecuritySignature /t REG_DWORD /d 1 /f`. Script all three changes and deploy via PSExec or a scheduled task. Note that disabling the `search:` URI handler will break Windows Search integration in Outlook and some Office features — document the functional impact before deploying in production.

Evidence: Before making registry changes, export and preserve: (1) `reg export HKCR\search search_uri_handler_baseline.reg` and `reg export HKCR\ms-search ms_search_uri_handler_baseline.reg` to document pre-remediation handler configuration and confirm whether the handler was tampered with by an attacker. (2) `reg export 'HKLM\SYSTEM\CurrentControlSet\Control\Lsa' lsa_auth_baseline.reg` to capture the pre-change LAN Manager authentication level. (3) Current SMB signing configuration: `Get-SmbClientConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature | Export-Csv smb_signing_baseline.csv`. These exports establish a configuration baseline for change management documentation and confirm attacker persistence mechanisms were not installed in the URI handler registry keys.

Step 4: Recovery — After controls are applied, validate outbound SMB block with a controlled test from an internal workstation to a monitored external IP on TCP 445. Confirm Group Policy NTLM settings have propagated (gpresult /r). Run a targeted hunt for any NTLMv2 authentication events to external IPs in the 30 days prior to control implementation to assess whether exploitation occurred before remediation. Reset credentials for any accounts showing anomalous NTLM authentication patterns. Reference: NIST IR-4, AU-6, D3-LAM (Local Account Monitoring).

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 AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Firewall block validation without enterprise tooling: from a test workstation, run `Test-NetConnection -ComputerName -Port 445` — a TCP connect timeout or 'TcpTestSucceeded: False' confirms the block is effective. For GPO propagation confirmation on individual hosts: `gpresult /r | findstr /i 'ntlm lm'`. For the 30-day retroactive NTLM hunt without a SIEM, run the PowerShell query from Step 2 against archived Security event logs on the DC (`\DC01\C$\Windows\System32\winevt\Logs\Security.evtx`) and filter for Logon Type 3 with 'NtLmSsp' targeting IPs outside the known internal subnet ranges. For accounts flagged as anomalous, force password reset via: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` and revoke all active Kerberos tickets with `klist purge` on affected endpoints.

Evidence: For any account that showed anomalous NTLM authentication to external IPs, collect before credential reset: (1) Full Security event log export from the domain controller covering the account's logon history for the 30-day lookback period, specifically Event IDs 4768 (Kerberos TGT request), 4776 (NTLM credential validation), and 4771 (Kerberos pre-auth failure) to establish whether the captured NTLMv2 hash was cracked and used for subsequent authentication. (2) Active Directory last logon timestamps: `Get-ADUser -Properties LastLogonDate, PasswordLastSet, BadLogonCount`. (3) Any SMB session logs from file servers showing access by the flagged account during the exposure window — check `Microsoft-Windows-SMBServer%4Security.evtx` on file servers for Event ID 551 (SMB session authentication) correlated to the account and timeframe.

Step 5: Post-Incident — Document this item as a permanent compensating control gap requiring annual review, since no patch is forthcoming. Add the outbound SMB block and NTLM restriction to your security

baseline and CIS benchmark validation (CIS 4.4, CIS 4.5). Review whether other Windows URI handlers (ms-word:, ms-excel:, ms-powerpoint:, mailto:) require similar audit — the structural weakness identified here applies broadly. Update your NTLM usage inventory and set a target date for Kerberos-only enforcement in line with NIST IA-8 and AC-17. Reference: NIST PM-6, CA-7, D3-CH.

NIST Phase: Post Incident

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

Controls: NIST CA-7 (Continuous Monitoring), NIST AC-17 (Remote Access), NIST IA-8 (Identification and Authentication — Non-Organizational Users), NIST AU-11 (Audit Record Retention), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Document the permanent compensating control gap in a risk register entry that includes: CVE-2026-33829 identifier, vendor declination date, compensating controls applied (outbound SMB block, URI handler registry disable, SMB signing), residual risk statement, and annual review date. For the URI handler audit of related protocols (ms-word:, ms-excel:, ms-powerpoint:, mailto:), run: `reg query HKCR /f 'URL Protocol' /s | findstr /i 'ms-word ms-excel ms-powerpoint mailto'` to enumerate registered handlers and their command targets — review each ShellCommand value for suspicious or unintended SMB-triggering paths. For Kerberos-only migration planning, generate an NTLM usage report from the DC Security log with: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4776} | Group-Object -Property {$_.Properties[1].Value} | Sort-Object Count -Descending` to identify which systems and services still depend on NTLM and must be migrated before enforcement.

Evidence: Preserve as long-term incident record: (1) The complete compensating control change log with timestamps, approvals, and GPO/registry export snapshots from Steps 3 and 4. (2) The retroactive 30-day NTLM authentication hunt results, win or loss — if no exploitation was detected, document the methodology and log sources reviewed so future auditors can validate the assessment. (3) A registry export of all Windows URI handlers in their post-remediation state: `reg export HKCR hkcr_uri_handlers_post_remediation.reg` — this serves as the new baseline for CIS benchmark validation and annual review comparison. (4) Vendor advisory or public disclosure documentation confirming Microsoft's formal declination to patch CVE-2026-33829, retained as justification for the permanent compensating control classification.

Detection Guidance

Primary detection vector is outbound SMB traffic from workstations to external IPs. Query firewall logs for TCP 445 egress to non-RFC1918 addresses and correlate with source workstation and user account. In SIEM, create a detection rule: Windows Security Event ID 4648 (Explicit Credential Logon) or Event ID 4624 (Successful Logon) with Logon Type 3 (Network) and Authentication Package = NTLM, where the target server IP is external or non-domain-controlled. Correlate event timestamp with firewall logs showing outbound TCP 445 to the same external IP within a 5-minute window. In EDR, create a behavioral rule: process tree where a browser (svchost.exe, iexplore.exe, chrome.exe, firefox.exe) or email client (outlook.exe) spawns a child process invoking the 'search:' or 'ms-search:' URI handler (examine command line for search: or ms-search: protocol invocation) followed by an outbound TCP 445 connection to an external IP within 30 seconds. Hunting hypothesis: identify any workstation that has generated outbound NTLM authentication (Event ID 4624 Type 3 with NTLM package) to an IP not in your known domain controller, file server, or approved external system inventory. Advanced: in network packet captures on internal egress segments, look for SMB NTLMSSP_AUTH message types that indicate NTLM handshakes; while the challenge-response itself is not plaintext, captured NTLM hashes are vulnerable to offline cracking or relay attacks. Relevant MITRE ATT&CK: T1187 (Forced Authentication) and T1557.001 (SMB Relay). Reference: NIST AU-6, AU-12, SI-4 (System Monitoring), CIS Controls v8.1 8.2.

Framework Mappings

MITRE-ATTACK

- **T1550.002** — Pass the Hash
- **T1071.002** — File Transfer Protocols
- **T1557.001** — LLMNR/NBT-NS Poisoning and SMB Relay
- **T1187** — Forced Authentication
- **T1566.002** — Spearphishing Link

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **SI-10** — Information Input Validation
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1550.002	Pass the Hash	Defense-Evasion
T1071.002	File Transfer Protocols	Command-And-Control
T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	Credential-Access
T1187	Forced Authentication	Credential-Access
T1566.002	Spearphishing Link	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/unpatched-windows-search-uri.html	T3
CVE-2026-33829 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-33829	T1
CVE-2026-33829 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-33829	T3
CVE-2026-33829: Snipping Tool NTLM Leak : r/blueteamsec - Reddit	https://www.reddit.com/r/blueteamsec/comments/1snmhzs/cve202633829_...	T3
Windows Snipping Tool Spoofing Bug Signals Early Patch Warning	https://windowsforum.com/threads/cve-2026-33829-windows-snipping-to...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33829, CVE-2023-35636	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3382...	T1

Generated 2026-06-03 13:58 UTC by TJS Security Command Center