INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

RegPwn (CVE-2026-24291): Windows Registry Accessibility Feature Privilege Escalation to SYSTEM

CVE VULNERABILITY | **CRITICAL**

SCC Item ID	SCC-CVE-2026-0019
Type	CVE Vulnerability
CVE ID	CVE-2026-24291
Severity	CRITICAL
EPSS Score	0.0006 (19th percentile)
Affected Products	Microsoft Windows (specific versions and builds not confirmed from verified sources at time of analysis)
Published	2026-03-18

Executive Summary

CVE-2026-24291 ('RegPwn') is a reported Windows privilege escalation vulnerability tied to the operating system's Accessibility feature registry handling, with claims of SYSTEM-level access achievable by a local attacker. At time of analysis, primary authorities (Microsoft MSRC and NIST NVD) have not published confirmed details, and source data originates solely from Tier 3 outlets; the critical severity rating and technical mechanism remain unverified. Organizations should monitor for official Microsoft and NIST advisories before committing remediation resources, while treating any SYSTEM-level local privilege escalation on Windows as high-priority if confirmed.

Technical Analysis

CVE-2026-24291 is classified under CWE-269 (Improper Privilege Management) and maps to MITRE ATT&CK techniques T1548 (Abuse Elevation Control Mechanism) and T1112 (Modify Registry). Reporting from Tier 3 sources (cyberpress.org) describes exploitation via Windows registry configurations associated with built-in Accessibility features, resulting in SYSTEM-level privilege escalation. The precise mechanism, whether improper access control, race condition, or registry key misconfiguration, has not been confirmed by Microsoft MSRC or NIST NVD as of 2026-03-04. Affected Windows versions and builds are unconfirmed from primary sources. CVSS base score is not yet published; EPSS score is 0.00061 (18.7th percentile), reflecting low observed exploitation probability at this time. CISA KEV inclusion has not occurred. NVD publication lag for 2026-vintage CVEs may account for the absence of primary-source data. No patch status or official advisory is

confirmed. Attack vector is assumed local (requires existing access to the target system) based on the privilege escalation classification, but this is not verified from primary sources.

Action Checklist

1. Step 1, Monitor primary sources: Check NIST NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-24291) and Microsoft MSRC (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24291) daily until official details are published; do not act on unverified severity claims.
2. Step 2, Assess exposure: Inventory Windows endpoints with Accessibility features enabled (Sticky Keys, Narrator, Magnifier, On-Screen Keyboard); these surfaces are consistent with the reported attack vector pending confirmation.
3. Step 3, Harden registry access controls: Audit and restrict write permissions on HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility and related subkeys to least-privilege accounts using Group Policy or registry ACL tooling.
4. Step 4, Enable and review telemetry: Ensure Windows Event Logging captures registry modification events (Event ID 4657) and process creation with elevated tokens (Event ID 4688 with privilege fields); baseline normal Accessibility-related registry activity now to support anomaly detection.
5. Step 5, Prepare patch response: Once Microsoft publishes an official advisory and patch, prioritize deployment on internet-exposed systems, privileged access workstations, and servers with interactive logon enabled; update internal vulnerability tracking and notify stakeholders at that time.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO/IR leadership immediately if (1) a confirmed exploit code or active exploitation is published for CVE-2026-24291, (2) internal threat intelligence or SOC detects suspicious Accessibility registry modifications or SYSTEM-level privilege escalation attempts from local accounts, or (3) Microsoft publishes a critical patch within 72 hours of advisory publication, indicating active threat in the wild.
Recovery Notes	After patch deployment and eradication of any confirmed exploitation, restore user access to Accessibility features as needed via Group Policy or registry ACL relaxation based on organizational requirements. Conduct post-incident forensic review of Event ID 4657, 4688, and 4670 logs covering 30 days prior to patch deployment to identify any undetected exploitation attempts or suspicious registry modifications. Update organization's vulnerability and incident response playbooks to reference this incident and the detection/containment controls deployed.
Forensic Artifacts	Windows Event Log 4657 (Registry Value Modified for HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility) | Windows Event Log 4688 (Process Creation with elevated tokens, especially sethc.exe, narrator.exe, magnify.exe, osk.exe spawned by non-standard parents) | Windows Event Log 4670 (Permissions on object changed for Accessibility registry keys) | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility registry hive exports and ACL snapshots | File system metadata and hash verification for sethc.exe, narrator.exe, magnify.exe, osk.exe (detection of backdoor replacement or modification)

Per-Action IR Details

Step 1 — Monitor primary sources: Check NIST NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-24291) and Microsoft MSRC (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24291) daily until official details are published; do not act on unverified severity claims.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: tools, resources, communication channels)

Controls: NIST 800-53 SI-5 (Security Alerts, Advisories, and Directives), CIS 3.14 (Maintain and regularly update asset inventory)

Compensating: Establish a daily check schedule using a shared calendar reminder. Designate one analyst to review NIST NVD and Microsoft MSRC at 08:00 UTC daily; document findings in a shared spreadsheet with columns for CVE, source, confirmed status, and action recommendation. Cross-reference with CISA KEV catalog (https://www.cisa.gov/known-exploited-vulnerabilities) at the same cadence.

Evidence: Capture baseline Windows registry snapshot for Accessibility-related keys (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility and subkeys) using `reg export` before any remediation to establish a forensic reference point for future anomaly comparison. Document all current ACLs using `icacls` command output.

Step 2 — Assess exposure: Inventory Windows endpoints with Accessibility features enabled (Sticky Keys, Narrator, Magnifier, On-Screen Keyboard); these surfaces are consistent with the reported attack vector pending confirmation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation: tools and resources for detection and containment); NIST 800-53 CM-8 (Information System Component Inventory)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 RA-3 (Risk Assessment), CIS 1.1 (Establish and maintain detailed asset inventory), CIS 6.2 (Monitor and control software installations)

Compensating: Use PowerShell WMI queries to remotely enumerate Accessibility feature status across your environment. Query `Get-WmiObject -Class Win32_Process -Filter 'Name="sethc.exe" OR Name="narrator.exe" OR Name="magnify.exe" OR Name="osk.exe"'` combined with registry queries via `reg query` (local or remote with `reg query \\\HKLM\...`). For air-gapped networks, export HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility registry export files from each endpoint using `reg export` and centralize for analysis in a spreadsheet. Cross-reference with Group Policy audit logs (Event ID 5136 from domain controllers) to identify policy-driven Accessibility feature deployments.

Evidence: Before querying, capture baseline process list snapshot (`tasklist /v`) and running service snapshot (`Get-Service | Export-Csv`) on a representative sample of endpoints. Document all Accessibility executables found with full file paths and timestamps. Export NTFS alternate data streams and file create/modify times for sethc.exe, narrator.exe, magnify.exe, osk.exe using `dir /s /a:hs` to detect any recent modifications or suspicious alternate streams. Capture Windows Defender scan logs and any third-party AV quarantine logs for Accessibility-related binaries.

Step 3 — Harden registry access controls: Audit and restrict write permissions on HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility and related subkeys to least-privilege accounts using Group Policy or registry ACL tooling.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation: tools and resources); NIST 800-53 AC-2 (Account Management), AC-6 (Least Privilege)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 AC-3 (Access Enforcement), CIS 5.3 (Manage administrator accounts)

Compensating: Use `icacls` to audit and modify registry ACLs on Accessibility keys. Command sequence: (1) Export current ACLs with `icacls "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility" /save

acl_backup.txt`; (2) restrict Write permissions to Administrators and SYSTEM only: `icacls "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility" /inheritance:r /grant:r "NT AUTHORITY\SYSTEM:(F)" /grant:r "BUILTIN\Administrators:(F)" /remove:g "Users"`; (3) audit the change with `icacls "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility"`; (4) for domain-joined systems, deploy via Group Policy Preferences (GPP) Registry or Security Group Policy Editor to apply at scale. Enable registry audit logging on modified keys using `auditpol /set /subcategory:"Registry" /success:enable /failure:enable` to monitor future modifications.

Evidence: BEFORE applying ACL changes: (1) Export current ACLs with `icacls ... /save` for all subkeys under Accessibility; (2) capture Windows Event Log 4657 (Registry Value Modified) for at least 7 days of baseline activity to understand legitimate Accessibility registry changes; (3) document all processes that write to these keys using Process Monitor (`procmon.exe`) capture with filter for registry write operations to Accessibility keys, run for 1 hour during normal business hours; (4) export NTFS file system ACLs for sethc.exe, narrator.exe, magnify.exe, osk.exe executables themselves using `icacls`.

Step 4 — Enable and review telemetry: Ensure Windows Event Logging captures registry modification events (Event ID 4657) and process creation with elevated tokens (Event ID 4688 with privilege fields); baseline normal Accessibility-related registry activity now to support anomaly detection.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis); NIST 800-53 AU-12 (Audit Generation), SI-4 (Information System Monitoring)

Controls: NIST 800-53 AU-12 (Audit Generation), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS 6.2 (Activate and manage monitoring and log collection)

Compensating: For systems without enterprise log aggregation: (1) Enable registry audit logging locally using `auditpol /set /subcategory:"Registry" /success:enable /failure:enable`; (2) configure Windows Event Log size and retention: `wevtutil sl Security /ms:1048576000` (1 GB retention); (3) export Event ID 4657 and 4688 daily using `wevtutil qe Security /q:*[System[(EventID=4657 or EventID=4688)]] /f:text > events_$(date +%Y%m%d).txt` and centralize to a shared folder or external drive; (4) manually parse exported logs weekly using `Select-String` PowerShell commands to identify registry modifications to Accessibility keys and suspicious elevated process creation; (5) establish a baseline by reviewing 30 days of activity and documenting all legitimate Accessibility registry paths and modification frequency.

Evidence: Capture 30-day baseline of Event ID 4657 and 4688 events BEFORE making any changes, to establish ground truth for normal Accessibility activity. Export full event details including User Account, Process Name, Process ID, Registry Path, Value Name, and Old Value/New Value. For Event ID 4688, ensure you enable privilege level capture by setting registry key: `HKLM\System\CurrentControlSet\Control\Lsa: AuditBaseObjects = 1` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit: ProcessCreationIncludeUserData = 1`. Capture baseline process snapshots for sethc.exe, narrator.exe, magnify.exe, osk.exe using Sysmon (if available) or Windows Defender Advanced Threat Protection (if licensed).

Step 5 — Prepare patch response: Once Microsoft publishes an official advisory and patch, prioritize deployment on internet-exposed systems, privileged access workstations, and servers with interactive logon enabled; update internal vulnerability tracking and notify stakeholders at that time.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery, post-incident activity); NIST 800-53 SI-2 (Flaw Remediation), CM-3 (Configuration Change Control)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-3 (Configuration Change Control), NIST 800-53 CM-4 (Security Impact Analysis), CIS 7.1 (Establish and maintain a patch management process)

Compensating: For teams without automated patch management: (1) Create a patch deployment checklist in a shared document listing all prioritized endpoints (use the inventory from Step 2); (2) before patch deployment, capture baseline registry export, Windows Event Log snapshot, and running process list for comparison post-patch using `reg export HKLM > baseline.reg`, `wevtutil export-log Security /filename:baseline.evtx`, and `tasklist /v > baseline.txt`; (3) deploy patch to test system first (non-production), monitor Event ID 4657 for registry changes during/after patch for 24

hours, and document any unexpected modifications; (4) deploy to production systems in waves: tier 1 = internet-facing systems first, tier 2 = privileged access workstations within 48 hours, tier 3 = remaining servers within 1 week; (5) after each wave, compare post-patch Event Logs and registry exports to baseline to detect any regression or unexpected behavior.

Evidence: Capture pre-patch baseline: registry exports, Event Log snapshots (4657, 4688, 4670), running processes, file hashes of Accessibility binaries using `certUtil -hashfile SHA256`. During patch deployment, enable verbose Windows Setup logging: `set SETUPETW=1` before running patch installer. After patch, compare hashes of modified system files, re-run registry ACL audit to confirm hardening remains in place, and review Event ID 4688 for any unexpected privilege escalation attempts during the patch window.

Detection Guidance

Detection is constrained by the absence of confirmed technical details. The following guidance is based on the reported CWE-269 classification and ATT&CK mappings (T1548, T1112) and should be treated as preparatory until primary-source confirmation is available. (1) Registry modification monitoring: Enable Object Access Auditing for the Accessibility-related registry paths (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility; HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout). Alert on Event ID 4657 where the modifying process is not a known system process (e.g., svchost.exe, winlogon.exe) or where the process runs under a standard user token. (2) Privilege escalation indicators: Monitor Event ID 4672 (Special privileges assigned to new logon) and Event ID 4624 (Logon Type 2 or 10) following unusual registry write activity. Correlate with Event ID 4688 to identify processes spawning with SYSTEM-level tokens from non-SYSTEM parent processes. (3) Accessibility feature abuse patterns: Alert on execution of accessibility binary replacements (e.g., sethc.exe, utilman.exe, narrator.exe, osk.exe) from unexpected parent processes or at the logon screen (winlogon.exe as parent). This is a known post-exploitation pattern consistent with T1546.008 and adjacent to the reported vector. (4) EDR/SIEM query sketch (pseudo-logic): process_parent = 'winlogon.exe' AND process_name IN ('cmd.exe','powershell.exe','mmc.exe'), flag for immediate review. No confirmed IOCs, hashes, or network indicators are available from verified sources at time of analysis.

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1112** — Modify Registry

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings

OWASP-TOP10-2021

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

CIS-V8

- **5.4**
- **6.8**

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1112	Modify Registry	Defense-Evasion

Sources

Source	URL	Tier
	https://cyberpress.org/regpwn-vulnerability/	T3
Act Fast! SMB Vulnerability Lets Attackers Gain SYSTEM-Level Access	https://www.secpod.com/blog/act-fast-smb-vulnerability-lets-attacke...	T3
CVE-2025-59287, Critical RCE in Windows Server Update Services	https://blog.senthorus.ch/posts/cve_2025_59287/	T3
U.S. CISA adds a flaw in Microsoft Windows to its Known Exploited ...	https://securityaffairs.com/186898/security/u-s-cisa-adds-a-flaw-in...	T3
CISA: High-severity Windows SMB flaw now exploited in attacks	https://www.bleepingcomputer.com/news/security/cisa-high-severity-w...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-24291	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-24291	T1

Generated 2026-03-29 18:43 UTC by TJS Security Command Center