INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-16 06:08 UTC

# CVE-2025-60710: Windows Task Host Privilege Escalation Confirmed Exploited, Five Months After Patch Release

**CVE VULNERABILITY** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CVE-2026-0042 |
| **Type** | CVE Vulnerability |
| **CVE ID** | CVE-2025-60710 |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **EPSS Score** | 0.1824 (95th percentile) |
| **Affected Products** | Windows 11, Windows Server 2025 (Microsoft) |
| **Published** | 2026-04-15T10:51:05 |
| **Discovery Source** | Rss |

## Executive Summary

A privilege escalation flaw in Windows Task Host (taskhostw.exe) was patched by Microsoft in November 2025 but is now confirmed under active exploitation, five months later. Attackers with any foothold on a Windows 11 or Windows Server 2025 system can use this vulnerability to gain full SYSTEM-level control, turning a limited compromise into a complete takeover. Organizations that have not applied the November 2025 patch are at elevated risk of full system compromise within ongoing intrusion campaigns.

## Technical Analysis

CVE-2025-60710 is a local privilege escalation vulnerability in taskhostw.exe affecting Windows 11 and Windows Server 2025. The root cause is improper link resolution before file access (CWE-59) combined with improper privilege management (CWE-269), enabling a low-complexity link-following attack. A local attacker with standard user privileges can escalate to SYSTEM without user interaction. CVSS base score: 7.5 (High). EPSS score: 0.182 (95th percentile), indicating high exploitation probability relative to all tracked CVEs. MITRE ATT&CK mappings: T1548 (Abuse Elevation Control Mechanism), T1574.010 (Services File Permissions Weakness), T1068 (Exploitation for Privilege Escalation). Microsoft issued a patch in November 2025 (Security Update Guide: msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710). CISA added the CVE to the

Known Exploited Vulnerabilities catalog on April 14, 2026, confirming in-the-wild exploitation. The five-month lag between patch release and KEV addition is consistent with post-initial-access use: attackers gain entry via another vector, then leverage this flaw to escalate privileges within the target environment. At the time of curation, NVD had not published a CVSSv3 vector string. Verify current vector at https://nvd.nist.gov/vuln/detail/CVE-2025-60710.

## Action Checklist

1. Containment, Identify all Windows 11 and Windows Server 2025 systems in your environment. Prioritize systems exposed to the internet or hosting sensitive workloads. Verify patch status against Microsoft's November 2025 Patch Tuesday update (KB article resolvable via msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710). Isolate any unpatched system with confirmed or suspected compromise.
2. Detection, Query endpoint detection logs for anomalous taskhostw.exe process behavior: unexpected child processes, privilege changes, or symbolic link creation by standard user accounts. Review Windows Security Event ID 4672 (Special Logon) and 4688 (Process Creation) for SYSTEM-level sessions preceded by standard-user activity on the same host. Search EDR telemetry for T1548 and T1068 execution patterns. The Vicarius detection script (vicarius.io/vsociety/posts/cve-2025-60710-detection-script-eop-vulnerability-in-host-process-for-windows-tasks) may assist host-level enumeration; treat as supplementary and validate before production deployment.
3. Eradication, Apply Microsoft's November 2025 cumulative update for Windows 11 and Windows Server 2025. Confirm patch installation via Windows Update history or your patch management console. If patching is not immediately possible, restrict standard user accounts from writing to directories resolvable by taskhostw.exe and enforce least-privilege access controls as a temporary compensating control.
4. Recovery, After patching, verify no SYSTEM-level sessions exist for accounts that should not hold that privilege. Run integrity checks on critical system files and scheduled tasks. Monitor Event ID 4672 and process creation logs for at least 72 hours post-remediation. Confirm taskhostw.exe is running as expected with no unusual parent-child process relationships.
5. Post-Incident, The five-month exploitation lag indicates your patch deployment cycle may have left a window. Audit patch SLA compliance for high and critical severity Microsoft updates. Review whether endpoint detection rules for T1068 and T1548 fired prior to KEV confirmation; if not, tune detection coverage. Consider privileged access workstation (PAW) controls and enforced least-privilege policies to reduce the blast radius of any future local privilege escalation exploits.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if Event ID 4672 or EDR telemetry confirms SYSTEM-level access on any host processing PII, PHI, PCI-DSS cardholder data, or regulated data subject to breach notification obligations, or if lateral movement indicators (e.g., Pass-the-Hash, remote scheduled task creation) are detected from a host where CVE-2025-60710 exploitation is suspected, indicating active intrusion campaign progression beyond the initial foothold. |

| | |
|---|---|
| **Recovery Notes** | After applying the November 2025 cumulative update, verify the patched taskhostw.exe binary hash matches the Microsoft-published value for the update and confirm no attacker-planted scheduled tasks persist in `C:\Windows\System32\Tasks\` by diffing against a known-good baseline. Monitor Windows Security Event IDs 4672 and 4688 continuously for a minimum of 72 hours post-patch, with specific focus on standard-user accounts that held any SYSTEM-level sessions during the exploitation window, as attackers may have established secondary persistence mechanisms (e.g., new local admin accounts, rogue scheduled tasks) before patching occurred. Any detection of SYSTEM-level privilege for non-service accounts during the monitoring window should be treated as evidence of persistent compromise and trigger a full re-scoping of the incident. |
| **Forensic Artifacts** | Windows Security Event Log (Security.evtx) — specifically Event ID 4672 (Special Logon) entries for non-service accounts receiving SeDebugPrivilege or SeTcbPrivilege, and Event ID 4688 (Process Creation) records showing taskhostw.exe as parent to cmd.exe, powershell.exe, or net.exe, which would indicate post-exploitation command execution under SYSTEM context via the CVE-2025-60710 privilege escalation path \| Scheduled task XML definitions at `C:\Windows\System32\Tasks\` and their corresponding registry entries under `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks` — taskhostw.exe is the host process for Windows Task Scheduler, making attacker-planted or modified task definitions a primary persistence artifact for this specific exploit class \| Prefetch files at `C:\Windows\Prefetch\TASKHOSTW.EXE-*.pf` and `C:\Windows\Prefetch\CMD.EXE-*.pf` — prefetch timestamps establish the execution timeline for taskhostw.exe and any processes it spawned, enabling reconstruction of the exploitation sequence and identification of tools executed under SYSTEM context \| Memory image of the affected system captured with WinPmem or Magnet RAM Capture — in-memory artifacts from taskhostw.exe exploitation may include injected shellcode, impersonation tokens, or symbolic link handle tables that are not recoverable from disk and are necessary to confirm the specific exploitation technique used against CVE-2025-60710 \| Windows Defender or EDR quarantine logs and process tree telemetry for the five-month window between the November 2025 patch release and KEV confirmation — these logs establish whether exploitation predated detection, the initial access vector that enabled an attacker to reach taskhostw.exe as a standard user, and the full scope of lateral movement or data access achieved after SYSTEM-level privilege was obtained |

### Per-Action IR Details

**Containment — Identify all Windows 11 and Windows Server 2025 systems in your environment. Prioritize systems exposed to the internet or hosting sensitive workloads. Verify patch status against Microsoft's November 2025 Patch Tuesday update (KB article resolvable via msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710). Isolate any unpatched system with confirmed or suspected compromise.**

**NIST Phase:** Containment

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

**Controls:** NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), 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 your environment via WinRM or local execution to enumerate unpatched Windows 11 and Server 2025 hosts — cross-reference output against the November 2025 KB: `Get-HotFix | Where-Object {$_.InstalledOn -gt '2025-10-31'} | Select-Object HotFixID, InstalledOn`. For hosts you cannot reach remotely, use a free Tenable Nessus Essentials scan (limited to 16 IPs) targeting the relevant KB check, or deploy osquery with the query `SELECT * FROM patches WHERE description LIKE '%CVE-2025-60710%';`. Isolate unpatched hosts at the switch/VLAN level or via Windows Firewall rules (`netsh advfirewall set allprofiles firewallpolicy

blockinbound,blockoutbound`) until patching is confirmed.

**Evidence:** Before isolating any host, preserve: (1) a full memory image using WinPmem or Magnet RAM Capture to capture any in-memory taskhostw.exe exploitation artifacts; (2) the Windows Security Event Log (Security.evtx) and System Event Log (System.evtx) exported via `wevtutil epl Security C:\evidence\Security.evtx`; (3) a snapshot of all running processes and their parent-child relationships via `Get-WmiObject Win32_Process | Select-Object Name, ProcessId, ParentProcessId, CommandLine | Export-Csv C:\evidence\processes.csv`; (4) current scheduled task definitions via `schtasks /query /fo LIST /v > C:\evidence\schedtasks.txt` since taskhostw.exe is the host process for scheduled tasks and may show tampered task definitions.

**Detection — Query endpoint detection logs for anomalous taskhostw.exe process behavior: unexpected child processes, privilege changes, or symbolic link creation by standard user accounts. Review Windows Security Event ID 4672 (Special Logon) and 4688 (Process Creation) for SYSTEM-level sessions preceded by standard-user activity on the same host. Search EDR telemetry for T1548 and T1068 execution patterns. The Vicarius detection script (vicarius.io/vsociety/posts/cve-2025-60710-detection-script-eop-vulnerability-in-host-process-for-windows-tasks) may assist host-level enumeration — treat as supplementary, validate before deployment in production.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1548 (Abuse Elevation Control Mechanism), MITRE ATT&CK T1068 (Exploitation for Privilege Escalation)

**Compensating:** Deploy Sysmon (free, Microsoft Sysinternals) with a configuration that enables Event ID 1 (Process Create) and Event ID 10 (ProcessAccess) — use the SwiftOnSecurity Sysmon config as a baseline. Then run this PowerShell query against Sysmon operational logs to surface anomalous taskhostw.exe children: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'taskhostw.exe' -and $_.Id -eq 1} | Select-Object TimeCreated, Message | Format-List`. For Event ID 4672/4688 hunting without a SIEM, use: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4672 -or $_.Id -eq 4688} | Where-Object {$_.Message -match 'taskhostw'} | Export-Csv C:\evidence\priv_events.csv`. Write a Sigma rule targeting taskhostw.exe spawning cmd.exe, powershell.exe, or whoami.exe for use with Hayabusa (free log analysis tool) against offline EVTX files.

**Evidence:** Collect before analysis: (1) Windows Security Event Log filtered for Event ID 4672 (Special Logon) entries where the account is not a known service account — these indicate unexpected SYSTEM token acquisition via taskhostw.exe exploitation; (2) Event ID 4688 (Process Creation) records showing taskhostw.exe as the parent process with child processes such as cmd.exe, powershell.exe, or net.exe; (3) Sysmon Event ID 1 logs showing command-line arguments for processes spawned under the SYSTEM SID that originated from a standard-user session; (4) Object access logs (Event ID 4663) for symbolic link creation or directory junction writes in paths accessible to taskhostw.exe, which is the likely exploitation mechanism for this class of privilege escalation; (5) Prefetch files at `C:\Windows\Prefetch\TASKHOSTW.EXE-*.pf` to establish execution timeline.

**Eradication — Apply Microsoft's November 2025 cumulative update for Windows 11 and Windows Server 2025. Confirm patch installation via Windows Update history or your patch management console. If patching is not immediately possible, restrict standard user accounts from writing to directories resolvable by taskhostw.exe and enforce least-privilege access controls as a temporary compensating control.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST AC-6 (Least Privilege), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** If the November 2025 cumulative update cannot be deployed immediately, use `icacls` to audit and restrict write permissions on directories that taskhostw.exe resolves at runtime — specifically user-writable paths in `%TEMP%`, `%APPDATA%`, and any paths surfaced in the scheduled task definitions: `icacls C:\Windows\System32\Tasks /remove:g 'BUILTIN\Users':(W)`. Additionally, use Group Policy (gpedit.msc on

standalone, or exported .pol files) to enforce 'Deny write access' for standard users on the Tasks directory. Enable Windows Defender Application Control (WDAC) in audit mode using the free Microsoft WDAC Wizard to log but not block suspicious process creation, providing visibility without requiring EDR. Verify patch deployment manually by running: `Get-HotFix -Id ` on each target system.

**Evidence:** Before patching, preserve: (1) a full export of all scheduled tasks (`schtasks /query /fo LIST /v`) to detect any attacker-planted persistence via the Task Scheduler that taskhostw.exe would execute post-exploitation; (2) registry export of `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks` and `\Tree` hives to capture task definitions that may not appear in the GUI; (3) file system timestamps (using `Get-ChildItem -Recurse C:\Windows\System32\Tasks | Select-Object FullName, LastWriteTime`) for any task XML files modified near the time of suspected exploitation; (4) a before-patch snapshot of `C:\Windows\System32\taskhostw.exe` hash via `Get-FileHash C:\Windows\System32\taskhostw.exe -Algorithm SHA256` to confirm the patched binary replaces the vulnerable version post-update.

**Recovery — After patching, verify no SYSTEM-level sessions exist for accounts that should not hold that privilege. Run integrity checks on critical system files and scheduled tasks. Monitor Event ID 4672 and process creation logs for at least 72 hours post-remediation. Confirm taskhostw.exe is running as expected with no unusual parent-child process relationships.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Run Windows System File Checker (`sfc /scannow`) to verify integrity of taskhostw.exe and related system binaries post-patch. Cross-check the SHA-256 hash of the patched `C:\Windows\System32\taskhostw.exe` against the value published in the Microsoft Security Update Guide for CVE-2025-60710. For scheduled task integrity, compare the post-patch `schtasks /query /fo LIST /v` output against the pre-incident baseline captured during eradication — diff the outputs using PowerShell: `Compare-Object (Get-Content baseline.txt) (Get-Content current.txt)`. For the 72-hour monitoring window without SIEM, run a scheduled PowerShell script every 15 minutes that queries Event IDs 4672 and 4688, appending results to a rolling log file for analyst review.

**Evidence:** Capture during recovery validation: (1) post-patch SHA-256 hash of `taskhostw.exe` to confirm the November 2025 patched binary is in place; (2) a current export of all scheduled task XML files from `C:\Windows\System32\Tasks\` compared against the pre-incident baseline to identify any attacker-planted persistence tasks that survived patching; (3) Event ID 4672 logs for the 72-hour monitoring window, filtered to flag any non-service accounts receiving SeDebugPrivilege or SeTcbPrivilege; (4) output of `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'} | Select-Object TaskName, TaskPath, State` to surface non-Microsoft tasks that may represent attacker persistence installed via the SYSTEM access gained through CVE-2025-60710 exploitation.

**Post-Incident — The five-month exploitation lag indicates your patch deployment cycle may have left a window. Audit patch SLA compliance for high and critical severity Microsoft updates. Review whether endpoint detection rules for T1068 and T1548 fired prior to KEV confirmation — if not, tune detection coverage. Consider privileged access workstation (PAW) controls and enforced least-privilege policies to reduce the blast radius of any future local privilege escalation exploits.**

**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-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** Conduct a lessons-learned review specifically measuring time-to-patch for the November 2025 Patch Tuesday cycle against your documented SLA for HIGH/CRITICAL severity Microsoft advisories — if no SLA exists, this incident is the forcing function to create one. Use the free CISA Known Exploited Vulnerabilities (KEV) catalog RSS

feed or API (`https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`) to automate alerting when any CVE affecting your Windows 11 or Server 2025 inventory enters the KEV catalog, providing a backstop for SLA failures. Write and deploy a Sigma rule targeting T1068 (taskhostw.exe spawning elevated child processes) into your log analysis pipeline using Hayabusa against historical EVTX archives to determine whether the exploitation was present before KEV confirmation and went undetected. Document PAW implementation requirements using the free Microsoft PAW guidance as the architecture reference.

**Evidence:** For the post-incident review, compile: (1) patch deployment timestamps from Windows Update logs (`C:\Windows\SoftwareDistribution\ReportingEvents.log`) across all affected hosts to quantify the actual exposure window between the November 2025 patch release and deployment completion; (2) historical Sysmon or Security Event Logs from the five-month window (November 2025 to the date of KEV confirmation) queried for T1548/T1068 indicators — specifically taskhostw.exe spawning elevated processes — to determine if exploitation predates your detection; (3) EDR or Windows Defender alert history for the same period to assess whether existing detection rules produced any signal for this technique prior to the incident; (4) a timeline reconstruction correlating Event ID 4688 process creation records with Event ID 4672 special logon events on affected hosts to establish the full scope of SYSTEM-level access obtained via CVE-2025-60710 during the exposure window.

## Detection Guidance

Focus detection on taskhostw.exe behavioral anomalies. Key signals: (1) taskhostw.exe spawning unexpected child processes or cmd.exe/powershell.exe as SYSTEM from a standard user session; (2) symbolic link creation (junction points or NTFS reparse points) in directories accessible by taskhostw.exe, logged via Windows object access auditing; (3) Windows Security Event ID 4672 showing SYSTEM-level special logon immediately following standard-user logon (Event ID 4624) on the same host; (4) Event ID 4688 with process creation showing elevated integrity level not consistent with the initiating user's token. In EDR tools, hunt for T1574.010 patterns: service binary or task host file path manipulation by a non-administrative account. The Vicarius detection script (vicarius.io, Tier 3 source) provides a host-based enumeration approach; treat as supplementary and validate before production deployment. EPSS of 0.182 at the 95th percentile confirms this CVE is in the actively exploited cohort; passive monitoring is insufficient for unpatched systems.

## Framework Mappings

### MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1574.010** — Services File Permissions Weakness
- **T1068** — Exploitation for Privilege Escalation

### NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IR-5** — Incident Monitoring

### OWASP-TOP10-2021

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

### CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### ISO-27001-2022

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

### NIST-CSF-2

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

### 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 |
| T1574.010 | Services File Permissions Weakness | Persistence |
| T1068 | Exploitation for Privilege Escalation | Privilege-Escalation |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/cisa-flags-windows-t... | T3 |
| **CVE-2025-60710 - CVE Record** | https://www.cve.org/CVERecord?id=CVE-2025-60710 | T3 |
| **Security Update Guide - Microsoft Security Response Center** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710 | T1 |
| **CVE-2025-60710 Detection Script - EoP Vulnerability in Host ...** | https://www.vicarius.io/vsociety/posts/cve-2025-60710-detection-scr... | T3 |
| **Microsoft Windows: CVE-2025-60710 - Rapid7 Vulnerability Database** | https://www.rapid7.com/db/vulnerabilities/microsoft-windows-cve-202... | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2025-60710 | T1 |

## DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-16 06:08 UTC by TJS Security Command Center