INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 18:55 UTC

Microsoft MDASH AI Discovers Two Critical RCE Flaws in Windows IKEv2 and TCP/IP Stacks (CVE-2026-33824, CVE-2026-33827)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0173
Type	CVE Vulnerability
CVE ID	CVE-2026-33824, CVE-2026-33827
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0010 (26th percentile)
Affected Products	Microsoft Windows, ikeext.dll (IKEv2 stack) affected by CVE-2026-33824; tcpip.sys (TCP/IP with IPSec + IPv6) affected by CVE-2026-33827
Published	2026-05-13T09:46:02
Discovery Source	Rss

Executive Summary

Microsoft patched two critical unauthenticated remote code execution vulnerabilities in core Windows networking components as part of the May 2026 Patch Tuesday cycle: CVE-2026-33824 (CVSS 9.8, IKEv2 stack in ikeext.dll) and CVE-2026-33827 (CVSS 8.1, TCP/IP stack with IPSec and IPv6 enabled in tcpip.sys). Both flaws require no user interaction and are reachable over the network, placing any enterprise running VPN, IPSec, or IPv6 infrastructure at direct risk of full system compromise. Organizations that delay patching face potential loss of network perimeter control, lateral movement into core infrastructure, and disruption of encrypted communications.

Technical Analysis

CVE-2026-33824 (CVSS 9.8) is a critical RCE in ikeext.dll, the Windows IKEv2 service component responsible for VPN and IPSec key exchange. An unauthenticated remote attacker can trigger the flaw with no user interaction over the network. CVE-2026-33827 (CVSS 8.1) is a high-severity RCE in tcpip.sys, exploitable when IPSec with IPv6 is enabled; it is similarly network-reachable and requires no authentication. Both were discovered by Microsoft's MDASH (Multi-agent Dynamic Analysis Scanning Harness) AI system and patched in the May 2026 Patch Tuesday release. Neither vulnerability is listed on the CISA KEV catalog as of this writing,

and EPSS scores are low (0.096% probability of exploitation in the next 30 days, 26th percentile), reflecting the absence of confirmed in-the-wild exploitation, not low severity. CWE classifications require per-CVE verification from NVD; preliminary mappings suggest CWE-415 (Double Free), CWE-362 (Race Condition), and CWE-787 (Out-of-Bounds Write) are relevant. MITRE ATT&CK techniques include T1210 (Exploitation of Remote Services), T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1203 (Exploitation for Client Execution), and T1068 (Exploitation for Privilege Escalation). Patch via May 2026 Patch Tuesday cumulative updates. Vendor advisories: MSRC CVE-2026-33824 and CVE-2026-33827 details at https://msrc.microsoft.com/update-guide/ and NVD at https://nvd.nist.gov/vuln/detail/CVE-2026-33824 and https://nvd.nist.gov/vuln/detail/CVE-2026-33827. Note: KB article numbers and exact build ranges should be confirmed against live records before operational deployment.

Action Checklist

1. Step 1: Containment. Identify all Windows systems running the IKEv2 service (ikeext.dll) and any systems with IPSec + IPv6 enabled on tcpip.sys. Prioritize internet-facing systems, VPN concentrators, and domain controllers. Apply network-level controls (firewall rules, ACLs) to restrict IKE (UDP 500, UDP 4500) and IPSec traffic to specific approved source IP addresses or networks only until the May 2026 Patch Tuesday update is deployed. Disable IPv6 on systems where it is not operationally required as a temporary measure for CVE-2026-33827 exposure.
2. Step 2: Detection. Query endpoint telemetry for unexpected ikeext.dll process crashes or restarts (Windows Event Log: System log, Event ID 7034/7031 for service crashes). Monitor for anomalous IKE negotiation traffic from external or unexpected IP addresses via network flow data and IDS/IPS signatures targeting IKEv2 fragmentation or malformed payloads. Review tcpip.sys-related crash dumps (WER logs, %SystemRoot%\Minidump) for evidence of memory corruption. Correlate with T1210 and T1190 detection logic in your SIEM.
3. Step 3: Eradication. Apply the May 2026 Patch Tuesday cumulative update to all affected Windows systems. Consult the Microsoft Security Update Guide at https://msrc.microsoft.com/update-guide/ and retrieve the specific KB article number(s) and affected build ranges from the CVE-2026-33824 and CVE-2026-33827 advisories. Validate patch application via Windows Update compliance reporting or your patch management platform. Re-enable IPv6 only after confirming the patch is applied.
4. Step 4: Recovery. After patching, verify ikeext service and tcpip.sys file versions match post-patch expectations. Restore any firewall rules or IPv6 configurations that were temporarily modified. Monitor IKE/IPSec tunnel re-establishment and confirm VPN functionality. Run a brief observation window (24-48 hours) on affected systems watching for anomalous network connections or service instability post-patch.
5. Step 5: Post-Incident Review. Review your patch SLA policy against the time from Patch Tuesday release to full deployment for CVSS 9.x flaws. Assess whether IKEv2 and IPSec services are appropriately segmented from direct internet exposure. Evaluate whether your detection coverage for memory corruption exploitation in Windows networking stacks is sufficient. Document this incident as a case study for vulnerability response timelines.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal/compliance immediately if any ikeext.dll or tcpip.sys crash dump analysis reveals shellcode artifacts, unexpected child processes, or outbound C2 connections from a VPN concentrator or domain controller, or if internet-facing systems were unpatched and exposed on UDP 500/4500 for more than 24 hours after Patch Tuesday release and processed traffic from non-whitelisted external peers — triggering potential breach notification assessment under applicable regulatory frameworks.
Recovery Notes	After deploying the May 2026 cumulative update, verify ikeext.dll and tcpip.sys file versions match the patched build specified in the MSRC advisory for CVE-2026-33824 and CVE-2026-33827 before re-enabling IPv6 or restoring unrestricted IKE/IPSec peering. Monitor the System Event Log for recurrence of Event ID 7031/7034 on ikeext and review IPSec SA establishment logs for unexpected peer IPs for a minimum of 48 hours post-patch, extending to 7 days on domain controllers and VPN concentrators given the full-system-compromise impact of pre-patch exploitation. Any system that exhibited ikeext or tcpip.sys crashes during the exposure window should be treated as potentially compromised until memory forensics clears the host.
Forensic Artifacts	Windows Error Reporting crash archives at %SystemRoot%\Minidump*.dmp and %ProgramData%\Microsoft\Windows\WER\ReportArchive\ — tcpip.sys or ikeext.exe fault buckets with bugcheck codes 0x50 or 0x7E indicate memory corruption consistent with CVE-2026-33824 or CVE-2026-33827 exploitation attempts | System Event Log (Event IDs 7031 and 7034) filtered to ikeext service — unexpected service crashes or restarts correlated with inbound IKEv2 traffic from external IPs are the primary host-side indicator of exploit delivery against CVE-2026-33824 | Network packet captures (PCAP) on UDP 500 and UDP 4500 from perimeter or host — malformed IKE_SA_INIT or CREATE_CHILD_SA payloads with anomalous fragmentation or oversized attributes are the network-layer artifact of CVE-2026-33824 exploit attempts; IPv6-encapsulated IPSec packets with fragmentation anomalies are the equivalent indicator for CVE-2026-33827 | Pre- and post-patch SHA-256 file hashes of C:\Windows\System32\ikeext.dll and C:\Windows\System32\drivers\tcpip.sys — unchanged hashes after claimed patch deployment indicate patch failure; hashes inconsistent with any known Microsoft-signed build version indicate potential binary tampering following exploitation | Volatile memory acquisition (winpmem or equivalent) from any host showing ikeext or tcpip.sys crashes during the exposure window — kernel-mode shellcode injected via a successful CVE-2026-33824 or CVE-2026-33827 exploit would reside in non-paged pool memory and will not survive reboot, making live memory forensics the only recovery path for implant detection on potentially compromised hosts

Per-Action IR Details

Step 1: Containment — Identify all Windows systems running the IKEv2 service (ikeext.dll) and any systems with IPSec + IPv6 enabled on tcpip.sys. Prioritize internet-facing systems, VPN concentrators, and domain controllers. Apply network-level controls (firewall rules, ACLs) to restrict IKE (UDP 500, UDP 4500) and IPSec traffic to known peers only until the May 2026 Patch Tuesday update is deployed. Disable IPv6 on systems where it is not operationally required as a temporary measure for CVE-2026-33827 exposure.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: Enumerate ikeext-running hosts with: `Get-Service -Name ikeext -ComputerName (Get-ADComputer -Filter *).Name | Where-Object {$_.Status -eq 'Running'}`. Block UDP 500 and UDP 4500 inbound from non-peer IPs using Windows Firewall via GPO: `netsh advfirewall firewall add rule name='Block IKE External' dir=in action=block

protocol=UDP localport=500,4500`. Disable IPv6 on all non-essential NICs via registry: `Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters' -Name 'DisabledComponents' -Value 0xFF`. Apply to a batch of systems using PSExec or Invoke-Command across targeted hosts.

Evidence: Before modifying firewall rules, capture existing Windows Firewall state (`netsh advfirewall show allprofiles`), current ikeext service status and binary hash (`Get-FileHash C:\Windows\System32\ikeext.dll`), and active IKE SA (Security Association) table via `netsh ipsec dynamic show all` to establish a pre-containment baseline. Capture running process list and network connections (`netstat -anob`) to detect any already-active anomalous IKE sessions from unexpected external peers that may indicate prior exploitation before containment was applied.

Step 2: Detection — Query endpoint telemetry for unexpected ikeext.dll process crashes or restarts (Windows Event Log: System log, Event ID 7034/7031 for service crashes). Monitor for anomalous IKE negotiation traffic from external or unexpected IP addresses via network flow data and IDS/IPS signatures targeting IKEv2 fragmentation or malformed payloads. Review tcpip.sys-related crash dumps (WER logs, %SystemRoot%\Minidump) for evidence of memory corruption. Correlate with T1210 and T1190 detection logic in your SIEM.

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 SI-4 (System Monitoring), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, deploy Sysmon with a config that includes Event ID 1 (Process Create) to catch any child processes spawned by ikeext.exe (which should never launch child processes under normal operation). Query System Event Log for ikeext crashes: `Get-WinEvent -LogName System | Where-Object {$_.Id -in @(7031,7034) -and $_.Message -like '*ikeext*'}`. For tcpip.sys kernel crashes, parse minidump metadata using the free `WinDbg Preview` (Microsoft Store) — look for `BugcheckCode 0x50 (PAGE_FAULT_IN_NONPAGED_AREA)` or `0x7E (SYSTEM_THREAD_EXCEPTION_NOT_HANDLED)` with tcpip.sys in the faulting module field. Use Wireshark with display filter `isakmp` to identify IKEv2 packets from non-whitelisted peers containing malformed or oversized fragmented payloads.

Evidence: Collect before triage: Windows Error Reporting crash archives at `%SystemRoot%\Minidump\*.dmp` and `%ProgramData%\Microsoft\Windows\WER\ReportArchive\` for tcpip.sys or ikeext.exe fault buckets; System Event Log entries with Event ID 7031 and 7034 filtered to ikeext service; network packet captures (PCAP) from the perimeter or host showing IKEv2 (UDP 500/4500) traffic from external IPs, specifically looking for malformed IKE_SA_INIT or CREATE_CHILD_SA payloads that could trigger the memory corruption in ikeext.dll (CVE-2026-33824) or the IPv6-encapsulated IPSec fragmentation anomalies that would trigger the tcpip.sys path for CVE-2026-33827.

Step 3: Eradication — Apply the May 2026 Patch Tuesday cumulative update to all affected Windows systems. Consult the Microsoft Security Update Guide at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824 and the corresponding CVE-2026-33827 advisory for specific KB article numbers and affected build ranges. Validate patch application via Windows Update compliance reporting or your patch management platform. Re-enable IPv6 only after confirming the patch is applied.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a patch management platform, script Windows Update deployment via PSWindowsUpdate module: `Install-Module PSWindowsUpdate; Get-WindowsUpdate -KBArticleID -Install -AutoReboot` executed remotely via Invoke-Command against your affected host list. After patching, verify ikeext.dll and tcpip.sys file versions against the post-patch build documented in the MSRC advisory using: `(Get-Item

C:\Windows\System32\ikeext.dll).VersionInfo.FileVersion` and `(Get-Item C:\Windows\System32\drivers\tcpip.sys).VersionInfo.FileVersion`. Cross-reference against the patched build number listed in the Microsoft Security Update Guide for the May 2026 cumulative update.

Evidence: Before deploying the patch, preserve a forensic image or at minimum file-level hashes of the vulnerable binaries: `Get-FileHash C:\Windows\System32\ikeext.dll -Algorithm SHA256` and `Get-FileHash C:\Windows\System32\drivers\tcpip.sys -Algorithm SHA256`. Retain pre-patch System Event Log exports and any WER crash reports as evidence of exploitation attempts. If any system showed ikeext or tcpip.sys crashes prior to patching, treat that host as potentially compromised and perform memory acquisition (`winpmem` or `RAMMap`) before patching to preserve volatile evidence of any injected shellcode in the IKEv2 or TCP/IP stack address space.

Step 4: Recovery — After patching, verify ikeext service and tcpip.sys file versions match post-patch expectations. Restore any firewall rules or IPv6 configurations that were temporarily modified. Monitor IKE/IPSec tunnel re-establishment and confirm VPN functionality. Run a brief observation window (24-48 hours) on affected systems watching for anomalous network connections or service instability post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Verify patched binary versions with the PowerShell version-check commands from Step 3. Confirm ikeext service is running cleanly post-restart: `Get-Service ikeext | Select-Object Status, StartType`. Re-enable IPv6 selectively and confirm IPSec SA re-establishment using `netsh ipsec dynamic show all` or `Get-NetIPsecMainModeSA` (PowerShell). During the 24–48 hour observation window, run a scheduled task every 15 minutes that logs `netstat -anob > C:\IR\netstat_$(Get-Date -f yyyyMMdd_HHmm).txt` to catch any unexpected post-patch lateral movement or callback sessions that could indicate a pre-patch compromise was not fully eradicated.

Evidence: Post-patch, collect: updated file hashes of ikeext.dll and tcpip.sys to confirm version change; Windows Update history log (`Get-WinEvent -LogName 'Microsoft-Windows-WindowsUpdateClient/Operational'`) confirming the May 2026 KB installed successfully; IPSec SA logs showing clean re-establishment of expected VPN tunnels only from authorized peers; and any new Event ID 7031/7034 entries in the System log that would indicate the patched ikeext service is still crashing, which would warrant escalation and deeper forensic analysis of the host for persistent implants.

Step 5: Post-Incident — Review your patch SLA policy against the time from Patch Tuesday release to full deployment for CVSS 9.x flaws. Assess whether IKEv2 and IPSec services are appropriately segmented from direct internet exposure. Evaluate whether your detection coverage for memory corruption exploitation in Windows networking stacks is sufficient. Document this event as a case study for AI-assisted vulnerability discovery — the MDASH disclosure model may accelerate the cadence of similar critical-class findings going forward.

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 RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a tabletop exercise scoped specifically to the scenario: unauthenticated RCE reaching a VPN concentrator or domain controller via UDP 500 before patch deployment. Use the free CISA Tabletop Exercise Packages (CTEPs) as a template. For detection gap analysis specific to memory corruption in kernel networking components, develop a Sigma rule targeting System Event Log Event ID 7034 with ServiceName='ikeext' and cross-correlate with inbound UDP 500/4500 traffic from non-peer IPs in your firewall logs — publish the rule to your internal detection library. Document the MDASH AI discovery model as a threat intelligence process note: if AI-assisted internal fuzzing produces critical-class CVEs at higher frequency, your patch SLA for CVSS 9.x+ kernel networking CVEs should target 48–72 hours for internet-facing systems, not the standard 30-day cycle.

Evidence: Compile the full incident timeline: first MSRC advisory publication timestamp, time to initial detection query execution, time to containment (firewall ACL deployment), and time to full patch validation across all affected hosts. Retain all System Event Log exports, WER crash archives, pre- and post-patch binary hashes, and network PCAP captures as a complete evidence package for the lessons-learned review. This package also serves as documentation supporting NIST IR-6 (Incident Reporting) obligations if any affected systems processed regulated data during the exposure window.

Detection Guidance

Primary detection focuses on two components: ikeext.dll (IKEv2) and tcpip.sys (TCP/IP with IPSec + IPv6). On Windows endpoints, query the System event log for Event IDs 7034 and 7031 (service crash and unexpected termination) attributed to the IKE and AuthIP IPsec Keying Modules service. Collect and analyze WER (Windows Error Reporting) crash dumps from %SystemRoot%\Minidump for memory corruption indicators in ikeext.dll or tcpip.sys. At the network layer, monitor IKE traffic (UDP 500, UDP 4500) for malformed or oversized negotiation payloads, unexpected IKE_SA_INIT floods, or negotiation attempts from unauthenticated external sources. For CVE-2026-33827, flag anomalous IPv6 traffic patterns on hosts where IPSec with IPv6 is active. SIEM correlation: map to ATT&CK T1210 (Exploitation of Remote Services), T1190 (Exploit Public-Facing Application), T1203 (Exploitation for Client Execution), and T1068 (Exploitation for Privilege Escalation) detection rules. No confirmed public IOCs (IPs, domains, hashes) are available for these CVEs at this time; detection should focus on behavioral and crash-based indicators rather than signature IOCs.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1046** — Network Service Discovery
- **T1133** — External Remote Services
- **T1203** — Exploitation for Client Execution
- **T1190** — Exploit Public-Facing Application
- **T1499.004** — Application or System Exploitation
- **T1595.002** — Vulnerability Scanning
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **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
- **A.5.23** — Information security for use of cloud services

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1210	Exploitation of Remote Services	Lateral-Movement
T1046	Network Service Discovery	Discovery
T1133	External Remote Services	Persistence
T1203	Exploitation for Client Execution	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1499.004	Application or System Exploitation	Impact
T1595.002	Vulnerability Scanning	Reconnaissance
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/microsofts-mdash-ai-system-finds-...	T3
CVE-2026-33824 Detail - NVD - NIST	https://nvd.nist.gov/vuln/detail/CVE-2026-33824	T1
Microsoft Security Update Guide - CVE-2026-33824	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824	T1
CVE-2026-33827 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-33827	T3
CVE-2026-33827 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33827	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33824, CVE-2026-33827	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3382...	T1

Generated 2026-05-13 18:55 UTC by TJS Security Command Center