INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-03 18:28 UTC

Wireshark 4.6.5: 43+ CVEs Patched Including Three Remote Code Execution Paths, Update Now

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0116
Type	CVE Vulnerability
CVE ID	CVE-2026-5409, CVE-2026-5408, CVE-2026-5406, CVE-2026-5407, CVE-2026-5299, CVE-2026-5401, CVE-2026-5402, CVE-2026-5404, CVE-2026-5403, CVE-2026-5405, CVE-2026-5654, CVE-2026-5655, CVE-2026-5657, CVE-2026-5656, CVE-2026-5653, CVE-2026-6538, CVE-2026-6537, CVE-2026-6536, CVE-2026-6535, CVE-2026-6534, CVE-2026-6533, CVE-2026-6532, CVE-2026-6531, CVE-2026-6530, CVE-2026-6529, CVE-2026-6528, CVE-2026-6527, CVE-2026-6526, CVE-2026-6525, CVE-2026-6524, CVE-2026-6523, CVE-2026-6521, CVE-2026-6520, CVE-2026-6519, CVE-2026-6522, CVE-2026-6870, CVE-2026-6869, CVE-2026-6868
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0001 (2th percentile)
Affected Products	Wireshark prior to 4.6.5; Windows installers include Npcap 1.87 and Qt 6.10.3
Published	2026-05-03T12:49:04
Discovery Source	Rss

Executive Summary

Wireshark 4.6.5 patches 43 or more vulnerabilities, including three confirmed remote code execution flaws in the TLS, SBC codec, and RDP dissectors. Any organization running Wireshark in SOC, forensics, or network analysis environments is affected. The business risk is targeted code execution against analyst workstations, systems that typically hold access to sensitive network data and investigation infrastructure. RCE classifications are based on vendor release notes; individual NVD records for the full CVE list were not independently verified.

Technical Analysis

Wireshark prior to 4.6.5 contains 43+ CVEs across multiple dissectors. Three confirmed RCE vulnerabilities are the highest-priority findings: CVE-2026-5402 (TLS dissector, heap-based buffer overflow, CWE-122),

CVE-2026-5403 (SBC codec, stack-based buffer overflow, CWE-121), and CVE-2026-5405 (RDP dissector, class unconfirmed pending NVD publication). Additional vulnerability classes include integer overflow (CWE-190), integer underflow (CWE-191), infinite loop (CWE-835), null pointer dereference (CWE-476), and uncontrolled resource consumption (CWE-400). Attack vector: a threat actor can craft malformed network packets or packet capture files that trigger parsing flaws when opened in Wireshark. MITRE ATT&CK relevance: T1203 (Exploitation for Client Execution), T1204.002 (Malicious File, analyst opens crafted .pcap), T1566.001 (Spearphishing Attachment, delivering malicious capture files). Affected: all Wireshark versions prior to 4.6.5. Windows installers bundle Npcap 1.87 and Qt 6.10.3. CVSS base: 7.5 (High) for the batch; individual RCE CVE scores pending full NVD publication. EPSS score is currently low (0.012 percentile), consistent with pre-exploitation data, not an indicator of low risk. Confidence note: RCE CVE-to-dissector mappings are sourced from vendor release notes and secondary reporting; spot-checks were performed on CVE-2026-5408 and CVE-2026-5404 via NVD. Full NVD records for the complete CVE list were not independently verified at analysis time.

Action Checklist

1. Containment: Identify all workstations running Wireshark prior to 4.6.5 in SOC, forensics, threat hunting, and network engineering environments. Restrict those systems from opening untrusted .pcap or capture files until patched. Do not open externally supplied capture files on unpatched hosts.
2. Detection: Query your asset inventory and endpoint management tools (SCCM, Intune, osquery, or similar) for Wireshark versions below 4.6.5. On Windows, check installed software for 'Wireshark' with file version less than 4.6.5.0. Review recent .pcap file opens on analyst workstations via EDR telemetry (file open events, process creation from Wireshark.exe) for anomalous behavior.
3. Eradication: Update to Wireshark 4.6.5 using the official installer from wireshark.org. Windows users: the 4.6.5 installer includes updated Npcap 1.87 and Qt 6.10.3; a clean reinstall is preferred over in-place upgrade where possible. Validate the installer hash against the official download page before deployment.
4. Recovery: After patching, confirm installed version via Help > About Wireshark or 'wireshark --version'. Verify Npcap version on Windows via the Npcap installer entry in Add/Remove Programs. Monitor EDR alerts on analyst workstations for one week post-patch for any delayed exploitation indicators.
5. Post-Incident: This release highlights the risk of running unpatched packet analysis tools on privileged analyst workstations. Review your software update cadence for security tooling. Consider implementing a policy requiring Wireshark updates within 72 hours of a release containing RCE-class CVEs. Evaluate whether analyst workstations have unnecessary outbound access that could facilitate lateral movement if compromised.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and initiate full IR if any analyst workstation running Wireshark prior to 4.6.5 shows Wireshark.exe spawning unexpected child processes, initiating outbound network connections, or if a crash dump is found in %LOCALAPPDATA%\CrashDumps for Wireshark.exe — these are indicators of successful RCE exploitation of the TLS, SBC codec, or RDP dissector vulnerabilities and the compromised workstation likely holds credentials and access to sensitive investigation infrastructure.

Recovery Notes	After confirming Wireshark 4.6.5 and Npcap 1.87 are installed on all affected hosts, validate that no analyst workstation in the pre-patch window opened a .pcap file from an external or untrusted source — if any did, treat that host as potentially compromised and conduct memory triage. Monitor analyst workstations via Sysmon for a minimum of seven days post-patch, specifically watching for Wireshark.exe child process creation and anomalous outbound connections that would indicate staged payloads from malicious capture files that were opened before the patch. Document the patch completion timestamp per host for NIST IR-5 (Incident Monitoring) records and use the exposure window data to refine the security tooling patch SLA policy.
Forensic Artifacts	Wireshark crash dump files at %LOCALAPPDATA%\CrashDumps\Wireshark.exe.*.dmp — a successful RCE exploit against the TLS, SBC codec, or RDP dissector would likely produce a crash dump on failed exploitation attempts before achieving code execution; these dumps contain heap memory that may show the malformed dissector payload. | Sysmon Event ID 1 (Process Creation) in Microsoft-Windows-Sysmon%4Operational.evtx filtered for ParentImage=Wireshark.exe with any child Image — legitimate Wireshark operation never spawns child processes during packet capture or file open, making any child process a near-certain RCE indicator specific to these dissector CVEs. | Windows Prefetch files at C:\Windows\Prefetch\WIRESHARK.EXE-*.pf — record the last eight execution timestamps and referenced file paths, allowing reconstruction of which .pcap files were loaded by the vulnerable Wireshark build during the exposure window, directly mapping to potential exploitation via malformed TLS handshake, SBC codec stream, or RDP protocol capture files. | Npcap driver event logs in the Windows System Event Log (Source: npcap or NPF) — the Npcap 1.87 update bundled in Wireshark 4.6.5 patches the underlying packet capture driver; anomalous driver load events or filter application failures on pre-patch hosts may indicate attempted exploitation of Npcap-layer vulnerabilities separate from the dissector RCEs. | Windows Security Event ID 4688 (Process Creation with command line) in Security.evtx on analyst workstations — captures the full command line of Wireshark.exe invocations including file paths of .pcap files opened, enabling retrospective identification of every potentially malicious capture file that was processed by a vulnerable dissector build during the exposure window.

Per-Action IR Details

Containment — Identify all workstations running Wireshark prior to 4.6.5 in SOC, forensics, threat hunting, and network engineering environments. Restrict those systems from opening untrusted .pcap or capture files until patched. Do not open externally supplied capture files on unpatched hosts.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: On Windows endpoints without EDR: run 'Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*Wireshark*"} | Select-Object Name,Version' via PowerShell remoting or SCCM script to enumerate vulnerable hosts. Enforce a Group Policy Software Restriction Policy or AppLocker rule blocking Wireshark.exe on unpatched hosts from accessing network shares where .pcap files are stored. Physically communicate to analysts via Slack/email that externally sourced capture files must not be opened until patch confirmation.

Evidence: Before restricting file opens, preserve the following: (1) Windows Security Event Log Event ID 4688 (Process Creation) showing Wireshark.exe invocations with command-line arguments referencing .pcap file paths — extract from C:\Windows\System32\winevt\Logs\Security.evtx; (2) Recent file system access timestamps on analyst workstation .pcap directories (e.g., %USERPROFILE%\Documents, shared forensic file stores) to identify which files were opened on unpatched Wireshark builds; (3) Prefetch files at C:\Windows\Prefetch\WIRESHARK.EXE-*.pf to

confirm execution history and last run timestamps before containment begins.

Detection — Query your asset inventory and endpoint management tools (SCCM, Intune, osquery, or similar) for Wireshark versions below 4.6.5. On Windows, check installed software for 'Wireshark' with file version less than 4.6.5.0. Review recent .pcap file opens on analyst workstations via EDR telemetry (file open events, process creation from Wireshark.exe) for anomalous behavior.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Without SCCM/Intune: use osquery with the query 'SELECT name, version, install_location FROM programs WHERE name LIKE "%Wireshark%";' deployed via osquery's distributed query interface across endpoints. For manual single-host checks: 'Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Where-Object {$_.DisplayName -like "*Wireshark*"} | Select DisplayName, DisplayVersion'. To detect suspicious post-exploitation behavior indicative of the RCE CVEs in the TLS, SBC codec, or RDP dissectors: deploy Sysmon (Event ID 1, Process Creation) and filter for Wireshark.exe spawning child processes (cmd.exe, powershell.exe, mshta.exe) — this would indicate successful RCE via a malicious capture file triggering the dissector vulnerability.

Evidence: Collect before analysis concludes: (1) Windows Registry key HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark capturing installed version string; (2) Sysmon Event ID 1 logs filtered for Wireshark.exe parent process with anomalous child processes, stored in Microsoft-Windows-Sysmon%4Operational.evtx; (3) Windows Security Event ID 4663 (Object Access) on directories containing analyst .pcap libraries to identify which specific capture files were accessed by Wireshark.exe prior to detection; (4) Network connection logs (Sysmon Event ID 3) for outbound connections initiated by Wireshark.exe — legitimate Wireshark traffic analysis does not require outbound connections from the Wireshark process itself, making any such events high-confidence RCE indicators.

Eradication — Update to Wireshark 4.6.5 using the official installer from wireshark.org. Windows users: the 4.6.5 installer includes updated Npcap 1.87 and Qt 6.10.3 — a clean reinstall is preferred over in-place upgrade where possible. Validate the installer hash against the official download page before deployment.

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-7 (Least Functionality), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without automated patch deployment: download the Wireshark 4.6.5 Windows installer from wireshark.org and verify the SHA-256 hash published on the official download page before distribution — use 'Get-FileHash .\Wireshark-4.6.5-x64.exe -Algorithm SHA256' in PowerShell and compare against the published digest. Perform a clean uninstall of the prior Wireshark version (including Npcap) via Add/Remove Programs before installing 4.6.5 to ensure the bundled Npcap 1.87 replaces older Npcap versions that may carry separate vulnerabilities. For Linux/macOS deployments, use the distribution package manager (apt, brew) and pin to >= 4.6.5.

Evidence: Before executing the reinstall, preserve: (1) A copy of the current Wireshark installation directory (typically C:\Program Files\Wireshark\) including wireshark.exe, all dissector .dll files for the TLS, SBC, and RDP dissectors (epan\dissectors\libwireshark.dll and associated plugin DLLs), and the Npcap installation at C:\Program Files\Npcap\ — these are the components containing the patched CVEs and may be needed for forensic comparison; (2) The currently installed Npcap version from HKLM\SOFTWARE\Npcap registry key before replacement; (3) Any crash dump files in %LOCALAPPDATA%\CrashDumps or %APPDATA%\Wireshark that may indicate prior exploitation attempts via malformed dissector input.

Recovery — After patching, confirm installed version via Help > About Wireshark or 'wireshark --version'. Verify Npcap version on Windows via the Npcap installer entry in Add/Remove Programs. Monitor EDR alerts

on analyst workstations for one week post-patch for any delayed exploitation indicators.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-2 (Flaw Remediation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without EDR for post-patch monitoring: deploy a Sysmon configuration with targeted rules for Wireshark.exe spawning unexpected child processes (Rule Type: ProcessCreate, ParentImage contains Wireshark.exe, Image not contains Wireshark.exe) and export daily to a centralized log file via 'wevtutil qe Microsoft-Windows-Sysmon/Operational /q:"*[EventData[Data[@Name=\'ParentImage\'] and contains(.,\'Wireshark\')]]" /f:text > sysmon_wireshark_daily.txt'. Also run 'wireshark --version' via scheduled task and compare output to expected string '4.6.5' to detect unauthorized downgrades or version tampering.

Evidence: During the monitoring window, collect: (1) Wireshark process creation events (Sysmon Event ID 1) for any Wireshark.exe invocations where the command line includes .pcap file paths originating from external or email-delivered sources, which may indicate delayed detonation of malicious capture files opened before patching; (2) Npcap driver events in the Windows System Event Log (Event Source: npcap) for driver crashes or unexpected packet filter loads that could indicate post-exploitation persistence via Npcap's kernel driver component; (3) Windows Security Event ID 4672 (Special Privileges Assigned) on analyst accounts during the monitoring window — Npcap operates at kernel level, and privilege escalation post-exploitation of the Npcap component would appear here.

Post-Incident — This release highlights the risk of running unpatched packet analysis tools on privileged analyst workstations. Review your software update cadence for security tooling. Consider implementing a policy requiring Wireshark updates within 72 hours of a release containing RCE-class CVEs. Evaluate whether analyst workstations have unnecessary outbound access that could facilitate lateral movement if compromised.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For the 72-hour RCE patch policy: create a CISA KEV and Wireshark security advisory RSS feed monitor (wireshark.org/security/ publishes advisories) and assign a named analyst to check it weekly; formalize the 72-hour SLA in the IR plan. For outbound access restriction on analyst workstations: apply Windows Firewall rules blocking all outbound connections from Wireshark.exe except to explicitly needed capture interfaces — 'netsh advfirewall firewall add rule name="Block Wireshark Outbound" dir=out program="C:\Program Files\Wireshark\Wireshark.exe" action=block' — to limit lateral movement potential if an RCE in a dissector like TLS or RDP is triggered via a malicious capture file.

Evidence: For the lessons-learned record, preserve: (1) The full software inventory snapshot from detection phase showing all hosts running vulnerable Wireshark versions and their exposure window (time between 4.6.5 release and patch confirmation); (2) Any .pcap files from external sources that were opened on analyst workstations during the vulnerability window — these should be quarantined and reviewed in a sandboxed environment for embedded malformed TLS, SBC, or RDP dissector payloads; (3) IR timeline documentation per NIST IR-5 (Incident Monitoring) capturing detection-to-patch intervals across all affected hosts for use in SLA gap analysis.

Detection Guidance

Primary detection method is version enumeration. Query endpoint management (SCCM, Intune, osquery) for Wireshark installs with version < 4.6.5. EDR behavioral query: look for Wireshark.exe process spawning child processes, making outbound network connections, or writing files to unexpected paths; these are not normal Wireshark behaviors and may indicate exploitation. For analyst environments that open external capture files,

review file provenance logs for .pcap or .pcapng files received via email or external transfer in the 30 days before patch. No public IOCs (IPs, domains, hashes) are associated with active exploitation of these CVEs at time of analysis. CISA KEV status is false and EPSS percentile is very low, suggesting no confirmed in-the-wild exploitation yet.

Framework Mappings

MITRE-ATTACK

- **T1499.004** — Application or System Exploitation
- **T1204.002** — Malicious File
- **T1203** — Exploitation for Client Execution
- **T1566.001** — Spearphishing Attachment

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SI-16** — Memory Protection
- **SC-5** — Denial-of-Service Protection
- **SC-13** — Cryptographic Protection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **13.8** — Deploy a Network Intrusion Prevention Solution
- **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

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499.004	Application or System Exploitation	Impact
T1204.002	Malicious File	Execution

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1566.001	Spearphishing Attachment	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.wireshark.org/docs/relnotes/wireshark-4.6.5.html	T3
CVE-2026-5408 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-5408	T1
Wireshark 4.6.x < 4.6.5 Multiple Vulnerabilities | Tenable®	https://www.tenable.com/plugins/nessus/311426	T3
Critical Wireshark Vulnerabilities Let Attackers Execute Arbitrary ...	https://hacklido.com/news/critical-wireshark-vulnerabilities-let-at...	T3
CVE-2026-5404 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-5404	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-5409, CVE-2026-5408, CVE-...	T1

Generated 2026-05-03 18:28 UTC by TJS Security Command Center