INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 19:31 UTC

Windows Dynamic Host Configuration Protocol (DHCP) Tampering Vulnerability

CVE VULNERABILITY | CRITICAL | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0280
Type	CVE Vulnerability
CVE ID	CVE-2026-45602
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Microsoft Windows 10 Version 1809 for 32-bit Systems (and likely broader Windows ecosystem, see note)
Published	2026-06-09T07:00:59
Discovery Source	Msrc Patch Tuesday

Executive Summary

Microsoft disclosed a critical tampering vulnerability (CVE-2026-45602, CVSS 9.1) in the Windows DHCP component as part of the June 2026 Patch Tuesday release. An attacker with network access could manipulate DHCP traffic to redirect clients, assign malicious DNS or gateway settings, and position themselves to intercept communications across the affected network segment. Organizations running unpatched Windows environments, particularly those with flat or poorly segmented networks, face elevated risk of man-in-the-middle attacks, credential interception, and broader lateral movement.

Technical Analysis

CVE-2026-45602 is a tampering vulnerability in the Windows DHCP component, assigned a CVSS base score of 9.1 (Critical). Associated weaknesses are CWE-923 (Improper Restriction of Communication Channel to Intended Endpoints) and CWE-290 (Authentication Bypass by Spoofing). MITRE ATT&CK techniques mapped to this vulnerability include T1557 (Adversary-in-the-Middle), T1557.003 (DHCP Spoofing), and T1565.002 (Transmitted Data Manipulation). Microsoft MSRC advisory confirms the affected product as Windows 10 Version 1809 for 32-bit Systems; broader Windows ecosystem impact stated by Microsoft has not been independently verified from accessible authoritative sources at this time. Specific exploit mechanics and proof-of-concept code have not been confirmed. EPSS score is not yet populated (0.0), suggesting limited observed exploitation data at time of disclosure. The vulnerability is not listed in the CISA KEV catalog. Active exploitation status is unknown. NVD has not yet published an independent CVSS vector or score; details above are sourced from MSRC disclosure. Analysts should verify details directly at the MSRC advisory

(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602) before acting on technical specifics.

Action Checklist

1. Step 1: Containment, Identify all Windows 10 Version 1809 (32-bit) systems running DHCP services or relying on DHCP in network segments accessible to untrusted hosts. Isolate high-value segments by enforcing DHCP snooping on managed switches to block rogue DHCP server responses until the Microsoft patch is applied. Consult the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602 to confirm the full affected product scope before scoping containment. References: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query DHCP server logs and Windows Event Logs for unexpected DHCP OFFER or ACK messages originating from non-authoritative servers (Event IDs 1024, 1025 vary by Windows version; filter DHCP service events in the System log under source 'DhcpServer' or 'Microsoft-Windows-DHCP-Server'). Monitor for clients receiving gateway or DNS assignments that differ from known-good configurations. Alert on ARP table anomalies or DNS resolution changes that could indicate successful man-in-the-middle positioning (T1557.003). References: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Apply the Microsoft June 2026 Patch Tuesday security update addressing CVE-2026-45602 to all affected Windows systems. Verify patch applicability against the full product list published in the MSRC advisory; do not assume coverage based solely on the confirmed Windows 10 1809 (32-bit) scope. Enable DHCP snooping and Dynamic ARP Inspection (DAI) on network infrastructure as a permanent compensating control where patching cannot be completed immediately. References: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patching, confirm DHCP service integrity by verifying that all clients are receiving gateway and DNS assignments from authoritative servers only. Review ARP tables and DNS cache on sampled endpoints to confirm no residual malicious assignments persist. Re-enable any isolated segments and confirm network path integrity. Continue monitoring DHCP and network traffic logs for at least 72 hours post-remediation. References: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
5. Step 5: Post-Incident, Assess whether network segmentation and DHCP snooping controls were in place before this disclosure; document gaps. Review the organization's patch cadence for critical Microsoft updates and confirm that Windows 10 1809 systems are still within supported lifecycle. If 1809 is approaching or past end-of-support, initiate an upgrade plan. Consider whether man-in-the-middle detection capabilities exist in current SIEM or NDR tooling. References: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal/compliance counsel immediately if forensic analysis of DHCP lease logs, ARP tables, or network packet captures confirms that a rogue DHCP server successfully issued malicious gateway or DNS assignments to any client — indicating active MitM positioning (T1557.003) that may have intercepted credentials, session tokens, or regulated data (PII/PHI/PCI) and could trigger breach notification obligations.
Recovery Notes	After patching CVE-2026-45602 and restoring segments, force a full DHCP lease renewal across all previously affected clients and validate that 'ipconfig /all' output confirms gateway and DNS values match authoritative server assignments with no residual attacker-controlled entries persisting in ARP or DNS cache. Conduct 72-hour continuous DHCP traffic monitoring via SPAN port packet capture (Wireshark filter: 'bootp') to confirm no rogue DHCP server re-emerges, particularly in network segments shared with untrusted or guest hosts. If Windows 10 1809 systems are confirmed end-of-support, treat them as permanently elevated risk and accelerate upgrade planning — patch availability for future DHCP-layer vulnerabilities cannot be assumed for unsupported builds.
Forensic Artifacts	Windows DHCP Server lease database files at C:\Windows\System32\dhcp\ (*.mdb, *.log) — preserves a record of all leases issued, including any attacker-issued leases with tampered option 3 (default gateway) and option 6 (DNS server) values that are the direct mechanism of CVE-2026-45602 exploitation | Windows System Event Log (EVTX) from DHCP server hosts filtered on source 'Microsoft-Windows-DHCP-Server' — captures DHCP OFFER and ACK events that would reveal unauthorized lease issuance from a rogue server operating via the CVE-2026-45602 tampering mechanism | Full PCAP of UDP port 67/68 traffic captured on a SPAN/mirror port of the affected segment — preserves raw DHCP OFFER frames containing attacker-controlled BOOTP option fields (gateway, DNS, NTP) that constitute the MitM redirect payload specific to this tampering vulnerability | ARP cache snapshots ('arp -a' output) collected from client endpoints in affected segments — reveals whether successful DHCP tampering led to attacker-controlled gateway MAC address entries, confirming T1557.003 MitM positioning achieved post-exploitation | DNS cache exports ('ipconfig /displaydns' on Windows clients) from endpoints in affected segments — identifies whether clients resolved hostnames through attacker-controlled DNS servers assigned via malicious DHCP ACK, indicating potential for credential or session interception downstream of the initial DHCP tampering

Per-Action IR Details

Step 1: Containment — Identify all Windows 10 Version 1809 (32-bit) systems running DHCP services or relying on DHCP in network segments accessible to untrusted hosts. Isolate high-value segments by enforcing DHCP snooping on managed switches to block rogue DHCP server responses until the Microsoft patch is applied. Consult the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602 to confirm the full affected product scope before scoping containment. References: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On managed switches (Cisco IOS example): enable 'ip dhcp snooping' globally, then apply 'ip dhcp snooping trust' only on uplink ports connected to the authoritative DHCP server — all client-facing ports remain untrusted, dropping rogue DHCP OFFERs. For teams without managed switch access, use a Windows host-based firewall rule to block inbound UDP 67/68 from non-authoritative server IPs: 'New-NetFirewallRule -DisplayName "Block Rogue DHCP" -Direction Inbound -Protocol UDP -LocalPort 67,68 -RemoteAddress -Action Block'. Wireshark capture

filter 'udp port 67 or udp port 68' on a trunk port can confirm whether rogue OFFER packets are present before switch changes are made.

Evidence: Before enforcing DHCP snooping, capture a full packet capture (PCAP) of DHCP traffic on the affected segment using Wireshark with display filter 'bootp' to preserve any rogue DHCP OFFER or ACK frames containing attacker-controlled gateway (option 3) or DNS (option 6) values. Export the current DHCP server lease database from the authoritative Windows DHCP Server (located at C:\Windows\System32\dhcp*.mdb or exportable via 'netsh dhcp server export C:\dhcp_backup.txt all') to establish a known-good baseline of issued leases before isolation disrupts normal traffic.

Step 2: Detection — Query DHCP server logs and Windows Event Logs for unexpected DHCP OFFER or ACK messages originating from non-authoritative servers (Event IDs vary by Windows version; filter DHCP service events in the System log under source 'DhcpServer' or 'Microsoft-Windows-DHCP-Server'). Monitor for clients receiving gateway or DNS assignments that differ from known-good configurations. Alert on ARP table anomalies or DNS resolution changes that could indicate successful man-in-the-middle positioning (T1557.003). References: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: On the authoritative Windows DHCP Server, run: 'Get-WinEvent -LogName System -FilterXPath "*[System[Provider[@Name=\'Microsoft-Windows-DHCP-Server\']]]" | Where-Object {$_.Message -match \'OFFER\' -or $_.Message -match \'ACK\'} | Export-Csv C:\dhcp_events.csv' to extract all DHCP service events. On client endpoints, run 'arp -a' and 'ipconfig /all' and compare gateway/DNS values against known-good configuration; script this across hosts with 'Invoke-Command -ComputerName -ScriptBlock {arp -a; ipconfig /all}'. Deploy the Sigma rule for MITRE T1557.003 (DHCP spoofing / adversary-in-the-middle) available in the SigmaHQ repository to parse Windows DHCP Server logs without a SIEM — execute via Chainsaw or Hayabusa against exported EVTX files.

Evidence: Collect Windows System Event Log (EVTX) from all hosts in the affected segment, specifically filtering for source 'Microsoft-Windows-DHCP-Server' events indicating lease grants to capture any attacker-issued ACKs with malicious option 3 (gateway) or option 6 (DNS) payloads. On affected clients, extract the ARP cache ('arp -a' output saved to file) and DNS cache ('ipconfig /displaydns' output) before any network changes, as these will reflect whether a client was successfully redirected to an attacker-controlled gateway or resolver. Additionally, collect NetFlow or switch MAC address table snapshots to identify the physical port and MAC address associated with any rogue DHCP server on the segment.

Step 3: Eradication — Apply the Microsoft June 2026 Patch Tuesday security update addressing CVE-2026-45602 to all affected Windows systems. Verify patch applicability against the full product list published in the MSRC advisory; do not assume coverage based solely on the confirmed Windows 10 1809 (32-bit) scope. Enable DHCP snooping and Dynamic ARP Inspection (DAI) on network infrastructure as a permanent compensating control where patching cannot be completed immediately. References: NIST SI-4 (no mapped control — SI-4 is outside the verified knowledge base control set; reference MSRC guidance directly), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For systems that cannot be patched immediately, enable Dynamic ARP Inspection (DAI) alongside DHCP snooping on managed switches (Cisco IOS: 'ip arp inspection vlan ') to prevent ARP poisoning that would follow a successful DHCP tampering attack. On the Windows DHCP Server itself, restrict the DHCP server service account to

minimum required privileges and confirm no unauthorized DHCP server instances are registered in Active Directory (run 'netsh dhcp show server' to enumerate all authorized DHCP servers in the domain — any unlisted server is suspect). Verify patch installation on each host using: 'Get-HotFix | Where-Object {$_.HotFixID -eq "KB"}' substituting the KB number from the MSRC advisory.

Evidence: Before applying the patch, image or snapshot the DHCP server's lease database (C:\Windows\System32\dhcp\ directory, including .mdb and .log files) and preserve Windows System Event Log EVTX from the DHCP server as forensic pre-patch baseline. Capture the output of 'netsh dhcp server show scope' and 'netsh dhcp server show optionvalue' to document any attacker-modified DHCP scope options (gateway, DNS, NTP) that may have been tampered with via CVE-2026-45602 before they are overwritten by patch remediation activity.

Step 4: Recovery — After patching, confirm DHCP service integrity by verifying that all clients are receiving gateway and DNS assignments from authoritative servers only. Review ARP tables and DNS cache on sampled endpoints to confirm no residual malicious assignments persist. Re-enable any isolated segments and confirm network path integrity. Continue monitoring DHCP and network traffic logs for at least 72 hours post-remediation. References: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Force all clients on previously affected segments to renew DHCP leases and flush DNS cache via GPO or script: 'ipconfig /release && ipconfig /renew && ipconfig /flushdns'. Validate that all renewed leases contain correct gateway and DNS values by running 'Invoke-Command -ComputerName -ScriptBlock {ipconfig /all | Select-String "Default Gateway","DNS Servers"}' and comparing output against the known-good configuration baseline captured in Step 1. Run a continuous Wireshark capture on a SPAN/mirror port for 72 hours post-recovery with display filter 'bootp' to confirm no rogue DHCP OFFERs re-emerge on the segment.

Evidence: Post-patch, collect renewed 'ipconfig /all' output and 'arp -a' snapshots from a representative sample of endpoints across each previously affected segment to confirm gateway and DNS assignments match authoritative server values. Preserve DHCP server lease database exports at 24-hour intervals during the 72-hour monitoring window to detect any anomalous lease issuance that might indicate persistence of a rogue DHCP server or re-exploitation attempt against other unpatched hosts in the broader Windows ecosystem.

Step 5: Post-Incident — Assess whether network segmentation and DHCP snooping controls were in place before this disclosure; document gaps. Review the organization's patch cadence for critical Microsoft updates and confirm that Windows 10 1809 systems are still within supported lifecycle. If 1809 is approaching or past end-of-support, initiate an upgrade plan. Consider whether man-in-the-middle detection capabilities exist in current SIEM or NDR tooling. References: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a lessons-learned review specifically examining: (1) whether DHCP snooping and DAI were absent from network switch configurations, (2) whether Windows 10 1809 systems appear in the asset inventory with lifecycle status flagged (CIS 1.1), and (3) whether the organization's patch SLA for CVSS 9.0+ Microsoft critical updates was met or exceeded. For ongoing DHCP-layer MitM detection without NDR tooling, deploy the open-source 'arpwatch' tool on a Linux host with a promiscuous-mode NIC on each segment to alert on MAC-to-IP binding changes that are a post-exploitation indicator of successful DHCP tampering (T1557.003).

Evidence: Preserve the complete incident timeline documentation including: initial detection timestamp, first evidence of rogue DHCP activity from EVTX exports, scope of affected clients (derived from DHCP lease database snapshots), and patch deployment completion records. These artifacts are required to support after-action reporting per NIST 800-61r3 §4 and may be required for regulatory notification assessments if intercepted traffic included PII or PHI handled on affected network segments.

Detection Guidance

Primary detection focus is rogue DHCP activity and downstream indicators of DHCP-based man-in-the-middle positioning. Query Windows System Event Log for DHCP-related events from the 'DhcpServer' or 'Microsoft-Windows-DHCP-Server' source; look for OFFER (Event ID 1024) or ACK (Event ID 1025) events from IP addresses not matching your authorized DHCP servers. On network infrastructure, enable DHCP snooping logs and alert on untrusted-port DHCP server packets. Monitor endpoint ARP caches for gateway MAC address changes that do not correspond to known infrastructure (T1557, T1557.003). Alert on DNS resolution anomalies - clients resolving known-good FQDNs to unexpected IPs may indicate successful gateway or DNS hijack via malicious DHCP assignment (T1565.002). Baseline authorized DHCP server IPs and lease ranges in your SIEM and alert on deviations. CIS 8.2 (Collect Audit Logs) requires that logging be confirmed enabled across enterprise assets before these queries are reliable. Consult Microsoft DHCP Event Log documentation for full Event ID reference and interpretation.

Framework Mappings

MITRE-ATTACK

- **T1557** — Adversary-in-the-Middle
- **T1557.003** — DHCP Spoofing
- **T1565.002** — Transmitted Data Manipulation

CIS-V8

- **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

NIST-800-53R5

- **IR-5** — Incident Monitoring

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access

Technique ID	Technique Name	Tactic
T1557.003	DHCP Spoofing	Credential-Access
T1565.002	Transmitted Data Manipulation	Impact

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45602	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Jun	T1
CVE-2026-27602 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-27602	T1
CVE-2026-45000: Openclaw SSRF Vulnerability in CDP Profile	https://www.sentinelone.com/vulnerability-database/cve-2026-45000/	T3
CVE-2026-41602 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-41602	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-45602	T1

Generated 2026-06-09 19:31 UTC by TJS Security Command Center