INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

Microsoft OOB Hotpatch Addresses RRAS Remote Code Execution Vulnerability in Windows 11 Enterprise

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0015
Type	CVE Vulnerability
CVE ID	CVE-2026-0015
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows 11 Enterprise (hotpatch update channel, versions 24H2 and 25H2); Microsoft Routing and Remote Access Service (RRAS)
Published	2026-03-16

Executive Summary

Microsoft issued an emergency out-of-band hotpatch (KB5084597) on March 14, 2026, to fix a remote code execution vulnerability in the Windows Routing and Remote Access Service (RRAS), affecting Windows 11 Enterprise 24H2 and 25H2 endpoints enrolled in the hotpatch update channel. The out-of-band release cadence signals Microsoft judged the risk urgent enough to bypass the standard Patch Tuesday schedule. Unpatched enterprise endpoints with RRAS exposed to the network are at risk of full remote compromise without user interaction. **ADVISORY STATUS: CVE identifier is pending MSRC publication. CVSS vector and EPSS score are unconfirmed. This item is sourced from secondary reporting only (T3 tier). Priority and detection guidance should be reassessed once MSRC publishes the canonical advisory with CVE ID assignment.**

Technical Analysis

KB5084597 addresses a remote code execution vulnerability in the Windows Routing and Remote Access Service (RRAS) on Windows 11 Enterprise versions 24H2 and 25H2 enrolled in the hotpatch update channel. Two CWE classes are associated: CWE-94 (Improper Control of Generation of Code) and CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), suggesting the vulnerability may involve memory corruption or code injection within the RRAS process. CVSS base score is reported at 7.5 (High); the CVSS vector is pending confirmation from MSRC advisory. No CVE identifier has been officially assigned in available source material at time of analysis; assignment is expected following MSRC publication. MITRE

ATT&CK techniques relevant to this vulnerability class include T1210 (Exploitation of Remote Services), T1133 (External Remote Services), and T1572 (Protocol Tunneling), reflecting RRAS's role in VPN and routing infrastructure. EPSS score and CISA KEV status are unconfirmed; no active exploitation has been disclosed in available sources. Attack surface is limited to endpoints enrolled in the hotpatch channel with RRAS running and network-accessible.

Action Checklist

1. Step 1 (Immediate): Verify KB5084597 deployment status on all Windows 11 Enterprise 24H2 and 25H2 endpoints enrolled in the hotpatch update channel. Prioritize systems where RRAS is active and network-exposed. Apply the patch immediately to any unpatched endpoints.
2. Step 2 (Detection): Query endpoint management tools (Intune, SCCM, or equivalent) for hotpatch enrollment status and KB5084597 installation confirmation. Cross-reference against your Windows 11 Enterprise 24H2/25H2 inventory.
3. Step 3 (Assessment): Identify all endpoints running RRAS. Assess whether RRAS is exposed to untrusted networks, particularly internet-facing or DMZ-adjacent systems. Prioritize those for immediate patching and interim network controls if patching is delayed.
4. Step 4 (Interim Control): If patching cannot be completed immediately, consider disabling RRAS on non-essential systems or restricting RRAS traffic at the network boundary using firewall ACLs or NSGs to reduce exposure surface.
5. Step 5 (Communication): Notify IT operations and endpoint management teams of the OOB release. Confirm patch deployment timelines with system owners for any deferred endpoints. Document exceptions with business justification.
6. Step 6 (Monitoring): Increase log retention and alerting sensitivity on RRAS-hosting systems for anomalous inbound connection attempts, unexpected process spawning from RRAS-related services (svchost hosting rasman/rras), or privilege escalation events. Update detection rules once MSRC publishes canonical CVE details and EPSS data.
7. Step 7 (Long-term): Review hotpatch channel enrollment coverage and patch SLA policies. Establish a process to track MSRC CVE publication and reassess priority once CVSS vector and EPSS data are confirmed by official advisory.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and IR leadership if any Windows 11 Enterprise 24H2/25H2 endpoint with RRAS remains unpatched and exposed to untrusted networks (including internet) for more than 48 hours after OOB release, or if evidence of exploitation attempts is detected in any RRAS event log, network flow, or IDS alert.
Recovery Notes	After patching and interim controls are lifted: (1) Disable enhanced RRAS logging and monitoring (reduce resource overhead post-recovery). (2) Review post-incident monitoring data (at 2-week mark) for any missed exploitation indicators; if found, escalate to forensics team for root-cause analysis. (3) Update incident response runbooks with lessons learned from this OOB deployment, including communication checklist and patch validation procedures.

Forensic Artifacts	Windows Security Event Log (Event ID 4688, 4624, 5156) — process creation, logon events, firewall allow rules | Routing and Remote Access Operational Event Log (Event IDs 20225, 20226, 20219, 20258) — RAS connection attempts, service state changes | Windows Update log (C:\Windows\Logs\WindowsUpdate\WindowsUpdate.log) — hotpatch deployment timestamps and status | Sysmon operational event log (Event ID 1, 3, 10, 11) — process creation with parent-child relationships, network connections, registry modifications | Firewall audit logs (netsh advfirewall show rule name=all, Event ID 5156/5157 in Security log) — inbound connection attempts to RRAS ports (443, 1194, 500, 4500) | RAS connection history (rasphone /showstatus output, C:\Windows\System32\LogFiles\RRAS\) — authentication attempts and active sessions | Network traffic capture (.etl or .pcap) on RRAS-hosting segments — identify unexpected inbound connections or command-and-control traffic post-exploitation | Process memory dumps of svchost.exe instances hosting rasman service — volatile indicators of exploitation (injected shellcode, unusual DLL loads)

Per-Action IR Details

Step 1 (Immediate): Verify KB5084597 deployment status on all Windows 11 Enterprise 24H2 and 25H2 endpoints enrolled in the hotpatch update channel. Prioritize systems where RRAS is active and network-exposed. Apply the patch immediately to any unpatched endpoints.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase; patch management and inventory control)

Controls: NIST 800-53 SI-2 (Flaw Remediation), CIS Controls v8 2.3 (Address Unauthorized Software), CIS Controls v8 3.10 (Disable Dormant Accounts)

Compensating: Use 'Get-HotFix' PowerShell cmdlet on each endpoint to query installed KB articles; pipe to CSV for triage: Get-HotFix | Where-Object {$_.HotFixID -eq 'KB5084597'} | Export-Csv hotpatch_status.csv. Cross-reference against Active Directory computer list using dsquery or ADO queries. For air-gapped networks, export inventory from WSUS server using: wuauclt /reportnow, then review %SystemRoot%\CCM\Logs\WUAHandler.log.

Evidence: Before patching, capture: (1) Windows Update event log (Application channel, Event ID 19, 20, 25 for update status); (2) Registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and scheduled tasks for persistence mechanisms; (3) Network baseline (netstat -ano | findstr :80,:443,:1194 to capture existing RRAS listeners); (4) Process snapshot using Get-Process -IncludeUserName for rasman.exe parent-child relationships.

Step 2 (Detection): Query endpoint management tools (Intune, SCCM, or equivalent) for hotpatch enrollment status and KB5084597 installation confirmation. Cross-reference against your Windows 11 Enterprise 24H2/25H2 inventory.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (detection and analysis; identifying and understanding indicators)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), CIS Controls v8 8.1 (Unified Endpoint Management), CIS Controls v8 8.2 (Address Unauthorized Software)

Compensating: If no MDM is in place, use Group Policy audit exports: gpresult /h report.html on each endpoint, extract applied policies. Query Windows Update history via: Get-WmiObject -Class Win32_QuickFixEngineering | ConvertTo-Csv > patches.csv. For heterogeneous environments, deploy a scheduled task (PowerShell script running as SYSTEM) to report patch status to a central log aggregation point (Splunk, ELK, syslog) every 12 hours.

Evidence: Before querying, preserve: (1) Intune/SCCM device compliance reports (export as baseline); (2) Windows Update Agent log (C:\Windows\Logs\WindowsUpdate\WindowsUpdate.log); (3) Task Scheduler history for update tasks; (4) Group Policy Operational event logs (Event ID 5312, 5313 for policy application failures that may explain deployment gaps).

Step 3 (Assessment): Identify all endpoints running RRAS. Assess whether RRAS is exposed to untrusted networks, particularly internet-facing or DMZ-adjacent systems. Prioritize those for immediate patching and

interim network controls if patching is delayed.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (asset inventory and risk prioritization)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 CA-8 (Security Assessments), CIS Controls v8 1.1 (Establish and Maintain Detailed Asset Inventory)

Compensating: Query RRAS service status across domain: use Invoke-Command with New-PSSession to run 'Get-Service -Name RemoteAccess' against endpoint lists. Parse output and correlate with network topology (VLAN assignments, DMZ status). Use netstat -ano and netsh advfirewall show rule name=all | findstr RRAS to identify listening ports. For zero-trust assessment, cross-reference against firewall rules: PowerShell: Get-NetFirewallRule -Direction Inbound | Where-Object {$_.Name -like '*RRAS*'} | Get-NetFirewallPortFilter.

Evidence: Capture before assessment: (1) System role indicators (Get-WindowsFeature | grep -i RRAS for role-based assessment); (2) Network interface bindings (ipconfig /all, route print); (3) Active listening sockets (netstat -anob output with process association); (4) Firewall inbound rules configured for RAS (Export-NetFirewallRule); (5) VPN connection history in Event ID 20225 (Routing and Remote Access operational log).

Step 4 (Interim Control): If patching cannot be completed immediately, consider disabling RRAS on non-essential systems or restricting RRAS traffic at the network boundary using firewall ACLs or NSGs to reduce exposure surface.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.5 (containment strategy; network segmentation)

Controls: NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS Controls v8 3.3 (Configure Data Access Control Lists), CIS Controls v8 12.3 (Segment Network Based on Sensitivity)

Compensating: Disable RRAS on non-critical systems via: Disable-WindowsOptionalFeature -Online -FeatureName RasSrv -NoRestart, then restart. For network-boundary controls on resource-constrained networks, use Windows Defender Firewall rules: netsh advfirewall firewall add rule name='Block_RRAS_Inbound' dir=in action=block protocol=tcp localport=443,1194 remoteip=0.0.0.0/0. For on-premises firewalls without NSG, configure ACLs blocking TCP 443, 1194, and UDP 500/4500 (IPSec) from untrusted segments. Document each interim control with rollback procedure and business owner sign-off.

Evidence: Before applying controls, snapshot: (1) Current RRAS service state and startup type (Get-Service RemoteAccess, Get-ItemProperty HKLM:\System\CurrentControlSet\Services\RemoteAccess | select Start); (2) Active RAS connections (rasphone /showstatus, RAS event log Event ID 20226); (3) Firewall baseline (Export-NetFirewallRule > baseline_rules.csv); (4) Network traffic baseline (netsh trace start capture=yes tracefile=rras_baseline.etl, let run 1 hour, netsh trace stop).

Step 5 (Communication): Notify IT operations and endpoint management teams of the OOB release. Confirm patch deployment timelines with system owners for any deferred endpoints. Document exceptions with business justification.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (tools and resources; communication protocols)

Controls: NIST 800-53 IR-4 (Incident Handling), CIS Controls v8 16.1 (Establish an Incident Response Program)

Compensating: Create incident ticket with OOB advisory metadata: CVE N/A, KB5084597, CVSS 7.5, affected versions 24H2/25H2, release date 2026-03-14. Use ticketing system or shared spreadsheet to track: endpoint name, RRAS status, patch date, owner approval, deferral reason (if applicable). Send notification via email with subject line '[URGENT] KB5084597 RRAS RCE Hotpatch Deployment Required by [DATE]' and include link to MSRC advisory. For deferred systems, require written business justification (template: system name | owner | reason | interim controls applied | target patch date) signed by manager.

Evidence: No forensic capture required for this communication step, but preserve: (1) Email notification send logs; (2) Ticket creation timestamps; (3) Owner acknowledgment signatures (screenshots or approval records); (4) List of deferred endpoints with documented justifications for audit trail.

Step 6 (Monitoring): Increase log retention and alerting sensitivity on RRAS-hosting systems for anomalous inbound connection attempts, unexpected process spawning from RRAS-related services (svchost hosting rasman/rras), or privilege escalation events. Update detection rules once MSRC publishes canonical CVE details and EPSS data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (detection; signature and anomaly-based analysis)

Controls: NIST 800-53 AU-12 (Audit Generation), NIST 800-53 IR-4 (Incident Handling), CIS Controls v8 8.5 (Collect Detailed Audit Logs)

Compensating: Enable Windows Event Logs: (1) Security (Event ID 4688 for process creation — enable command-line auditing via Group Policy 'Audit process creation' and 'Audit: Audit the use of Backup Restore privilege'); (2) System (Event ID 7001/7002 for service startup); (3) Routing and Remote Access operational log (rasman Event IDs 20225, 20226, 20219); (4) Sysmon (if available) for parent-child process relationships. For log retention, set minimum 90 days: wevtutil sl Security /ms:104857600 /rt:true (100 MB with overwrite protection). Create manual detection rules using log parsing: search for rasman.exe spawning child processes like cmd.exe, powershell.exe, or unusual network utilities (Process.ParentImage contains 'rasman' AND Process.Image NOT IN [expected_list]); search for inbound TCP connections to ports 443, 1194 from external segments with Event ID 4624 (logon success) correlation.

Evidence: Immediately configure and retain: (1) Windows Security Event Log (minimum 30-day retention; enable archival if capacity limited); (2) Routing and Remote Access Operational event log; (3) Sysmon operational log (if deployed); (4) Process creation audit events (Event ID 4688); (5) Network connection events (Event ID 5156 Firewall Allow); (6) Privilege escalation events (Event ID 4688 with elevated token elevation type); (7) RAS activity logs at C:\Windows\System32\LogFiles\RRAS\ if applicable.

Step 7 (Long-term): Review hotpatch channel enrollment coverage and patch SLA policies. Establish a process to track MSRC CVE publication and reassess priority once CVSS vector and EPSS data are confirmed by official advisory.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (post-incident activities; lessons learned and process improvement)

Controls: NIST 800-53 CA-2 (Security Assessments), NIST 800-53 IR-2 (Incident Response Training), CIS Controls v8 2.1 (Enable and Enforce Automatic Software Updates)

Compensating: Establish recurring MSRC monitoring: subscribe to Microsoft Security Update Guide RSS feed (https://msrc.microsoft.com/update-guide/rss) or use free MSRC API (https://api.msrc.microsoft.com/). Create monthly patch review process: (1) Extract published CVEs with CVSS and EPSS scores; (2) Prioritize using CVSS severity + EPSS percentile (e.g., CVSS 7.0+ AND EPSS >60th percentile = immediate); (3) Cross-reference against inventory of affected products; (4) Document SLA: e.g., 'Critical/Immediate patches within 7 days; High within 14 days; Medium within 30 days.' Review hotpatch enrollment: audit which device groups are enrolled (Intune/SCCM), identify gaps (e.g., branch offices, VPN-only endpoints), document coverage percentage by business unit. Conduct annual patch SLA review and update based on OOB incidents like this one.

Evidence: Preserve for post-incident review: (1) This incident ticket and timeline; (2) Patch deployment logs (Windows Update logs, SCCM/Intune deployment history); (3) Monitoring alerts generated during response (to validate detection rules); (4) Communication trail (notifications sent, approvals, deferral justifications); (5) List of endpoints that were unpatched at time of OOB release (for gap analysis).

Detection Guidance

No IOCs or confirmed exploitation indicators are available in current sources. Detection should focus on behavioral and telemetry signals. (1) Confirm patch status: query Windows Update logs (%SystemRoot%\SoftwareDistribution\ReportingEvents.log) or use 'Get-HotFix -Id KB5084597' via PowerShell across enrolled endpoints. (2) Monitor Windows Event Log for RRAS-related anomalies: Event IDs 20227,

20228 (RAS connection failures), and unusual entries under the RemoteAccess source in the System log. (3) Watch for unexpected process creation under svchost.exe instances hosting RasMan or RemoteAccess services, particularly spawning cmd.exe, powershell.exe, or network utility processes. (4) Review network logs for unexpected inbound connections to TCP/UDP ports associated with RRAS (e.g., TCP 1723 for PPTP, UDP 500/4500 for IKEv2, TCP/UDP 1701 for L2TP). (5) Once the CVE identifier is published by MSRC with accompanying CVSS vector and threat intelligence, cross-reference against emerging exploitation activity and update detection rules accordingly. **Source Quality Note:** This item is sourced from tier T3 (secondary reporting) only. Detection posture and priority scoring should be updated when MSRC publishes the canonical advisory with CVE ID, CVSS vector, and vendor-confirmed details.

Framework Mappings

MITRE-ATTACK

- **T1572** — Protocol Tunneling
- **T1210** — Exploitation of Remote Services
- **T1133** — External Remote Services

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-16** — Memory Protection
- **SI-10** — Information Input Validation
- **SI-7** — Software, Firmware, and Information Integrity

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10**
- **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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1572	Protocol Tunneling	Command-And-Control
T1210	Exploitation of Remote Services	Lateral-Movement
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com	T3
Microsoft releases Windows 11 OOB hotpatch to fix RRAS RCE flaw	https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-...	T3
Microsoft Delivers Windows 11 Hotpatch for RRAS Code Execution ...	https://www.guru3d.com/story/microsoft-delivers-windows-11-hotpatch...	T3
Microsoft: Out-of-band update for hotpatch Windows 11 | heise online	https://www.heise.de/en/news/Microsoft-Out-of-band-update-for-hotpa...	T3
KB5084597: Microsoft outs Windows 11 25H2, 24H2 emergency ...	https://www.neowin.net/news/kb5084597-microsoft-outs-windows-11-25h...	T3

Generated 2026-03-29 18:40 UTC by TJS Security Command Center