INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 14:28 UTC

Microsoft Patches Critical Zero-Click Outlook Vulnerability Threatening Enterprises

CVE VULNERABILITY | CRITICAL | CVSS 9.0

SCC Item ID	SCC-CVE-2026-0166
Type	CVE Vulnerability
CVE ID	CVE-2026-40361
Severity	CRITICAL
CVSS Base Score	9.0
EPSS Score	0.0006 (18th percentile)
Affected Products	Microsoft Outlook (specific versions not confirmed from available sources)
Published	7 hours ago
Discovery Source	Serper

Executive Summary

Microsoft has patched CVE-2026-40361, a critical remote code execution vulnerability in Outlook that requires no user interaction to exploit. An attacker can compromise a system by sending a specially crafted email before the recipient opens or reads it. Given Outlook's near-universal deployment across enterprise environments, the attack surface is exceptionally broad. Organizations that have not applied the latest Microsoft patch are at immediate risk of full system compromise through standard email delivery.

Technical Analysis

CVE-2026-40361 is a critical zero-click remote code execution vulnerability in Microsoft Outlook. Exploitation requires no user interaction; a specially crafted email delivered to the target is sufficient to trigger code execution. Root cause is classified under CWE-122 (Heap-based Buffer Overflow) and CWE-94 (Improper Control of Code Generation), indicating memory corruption leading to arbitrary code execution. MITRE ATT&CK coverage maps to T1566.001 (Email-based delivery of crafted message, note: zero-click variant does not require user interaction), T1203 (Exploitation for Client Execution), and T1059 (Command and Scripting Interpreter execution post-compromise). CVSS base score is reported at 9.0 (Critical). EPSS score is 0.00058 (approximately 0.06%, 17th percentile) as of disclosure, indicating low current exploitation probability at the time of advisory publication, though this metric is expected to rise as the vulnerability is publicized. The CVE does not appear in CISA KEV at this time. Affected version ranges and the official CVSS vector string are not confirmed from available sources; consult the Microsoft Security Response Center advisory at

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361 [URL requires live verification] and NVD at https://nvd.nist.gov/vuln/detail/CVE-2026-40361 [URL requires live verification] for authoritative version scope. No threat actor attribution has been confirmed. Verification note: MSRC and NVD URLs require confirmation against live pages before operational use. Recommend validation before finalizing version scope and patch KB article numbers for deployment.

Action Checklist

1. Step 1: Containment. Identify all hosts running Microsoft Outlook across your environment using asset inventory or endpoint management tooling. Prioritize systems where Outlook is internet-facing or where email is delivered directly from external sources without inline inspection. Consult the official MSRC advisory [verify URL is live: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361] to confirm affected version ranges and isolate or restrict email delivery to unpatched systems if patching cannot be completed immediately.
2. Step 2: Detection. Query endpoint detection and response (EDR) telemetry for anomalous child process creation from OUTLOOK.EXE. Review Exchange and email gateway logs for inbound messages with malformed MIME structures, oversized headers, or unusual encoding patterns consistent with crafted payloads. Monitor for T1059-associated activity (script interpreter invocations) spawned from Outlook process trees. No confirmed IOC hashes or network indicators are available; focus on behavioral detection (see Detection Guidance section).
3. Step 3: Eradication. Apply the Microsoft patch released for CVE-2026-40361 via Windows Update, Microsoft Update Catalog, or your enterprise patch management platform. Specific KB article and patch ID should be confirmed directly from the official MSRC advisory. For environments where patching is delayed, consider disabling automatic email preview rendering in Outlook as a temporary mitigation, and enforce email inspection at the gateway to strip or quarantine anomalous message structures.
4. Step 4: Recovery. After patching, verify patch installation via endpoint management console or registry key confirmation per MSRC guidance. Re-enable any email delivery restrictions applied as temporary containment. Monitor Outlook process behavior for 72 hours post-patch for residual anomalous activity. Confirm no lateral movement occurred on systems that were exposed and unpatched during the window between disclosure and patch application.
5. Step 5: Post-Incident. Review your patch deployment SLA for critical Microsoft Office/Outlook CVEs and evaluate whether the time-to-patch target was met. Assess whether email security gateway controls (sandboxing, MIME inspection, attachment stripping) would have reduced exposure during the patch gap. Map control gaps to NIST SP 800-53 controls SI-2 (Flaw Remediation) and SI-3 (Malicious Code Protection). Consider adding zero-click Outlook exploitation to your threat hunting hypothesis backlog for future proactive hunts.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal counsel immediately if any Outlook host shows evidence of OUTLOOK.EXE spawning child processes, unexpected scheduled task creation, or new local administrator accounts during the exposure window — these indicators suggest successful RCE exploitation and may trigger breach notification obligations under GDPR, HIPAA, or state privacy laws if the compromised host processed PII or PHI.
Recovery Notes	After confirming patch installation via ClickToRun VersionToReport or KB package registry verification, restore email delivery incrementally — beginning with gateway-inspected internal traffic before re-enabling direct external SMTP delivery. Monitor Sysmon Event ID 1 for OUTLOOK.EXE parent process chains continuously for a minimum of 72 hours post-patch, as delayed-execution payloads or persistence mechanisms installed during the exposure window may activate after email flow resumes. If any host showed behavioral indicators of compromise during the exposure window, treat it as a full compromise and reimage rather than patch-in-place, per NIST 800-61r3 §3.4 eradication guidance.
Forensic Artifacts	Raw MIME source of inbound emails delivered during the exposure window, extracted from Exchange Recoverable Items or transport dumpster — the crafted message triggering CVE-2026-40361 is the primary exploit artifact and must be preserved before any mailbox remediation | Sysmon Event ID 1 (Process Create) records where ParentImage = OUTLOOK.EXE, capturing any child process spawned without user interaction — the definitive behavioral indicator of zero-click RCE exploitation for this vulnerability | Windows Security Event ID 4688 (Process Creation) with full command-line logging enabled, filtered on processes spawned from the OUTLOOK.EXE process tree during the exposure window, to reconstruct the attacker's initial execution chain | Outlook add-in registry keys at HKCU:\Software\Microsoft\Office\Outlook\Addins and HKLM:\SOFTWARE\Microsoft\Office\Outlook\Addins, and the corresponding DLL files in those paths — a successful RCE exploit against Outlook commonly establishes persistence via malicious COM add-in registration | Memory dump of the OUTLOOK.EXE process (via ProcDump -ma) captured on any host exhibiting anomalous child process creation, preserving potential shellcode, injected PE reflections, or heap spray artifacts deposited by the zero-click exploit payload before the process terminates or is patched

Per-Action IR Details

Step 1: Containment — Identify all hosts running Microsoft Outlook across your environment using asset inventory or endpoint management tooling. Prioritize systems where Outlook is internet-facing or where email is delivered directly from external sources without inline inspection. Consult the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361) to confirm affected version ranges and isolate or restrict email delivery to unpatched systems if patching cannot be completed immediately.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'wmic product where name like "%Outlook%" get name,version,installdate /format:csv > outlook_inventory.csv' or use PowerShell 'Get-ItemProperty HKLM:\Software\Microsoft\Office*\Outlook\InstallRoot' across all endpoints via PSExec or WinRM sweep. For email gateway isolation without enterprise tooling, configure an on-premises Exchange transport rule or MX-level hold to quarantine all inbound external SMTP for unpatched hosts identified in the sweep. Use osquery with 'SELECT name, version FROM programs WHERE name LIKE "%Outlook%"' for cross-platform inventory if osquery agents are deployed.

Evidence: Before isolating any host, capture a full list of recently received emails from the Exchange transport log at '%ExchangeInstallPath%\TransportRoles\Logs\Hub\Connectivity\' and the SMTP receive logs, filtering on the 24–72 hours prior to patch availability. Preserve the Outlook NK2/autocomplete cache at

'%APPDATA%\Microsoft\Outlook*.dat' and the OST/PST file timestamps, which may reflect message arrival times consistent with pre-open exploitation. Document the Outlook build version from HKLM:\SOFTWARE\Microsoft\Office\ClickToRun\Configuration (VersionToReport) on each host before any remediation action alters registry state.

Step 2: Detection — Query endpoint detection and response (EDR) telemetry for anomalous child process creation from OUTLOOK.EXE. Review Exchange and email gateway logs for inbound messages with malformed MIME structures, oversized headers, or unusual encoding patterns consistent with crafted payloads. Monitor for T1059-associated activity (script interpreter invocations) spawned from Outlook process trees. No confirmed IOC hashes or network indicators are available at this time; focus on behavioral detection.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config) and query for Event ID 1 (Process Create) where ParentImage ends in 'OUTLOOK.EXE' and Image matches cmd.exe, powershell.exe, wscript.exe, cscript.exe, mshta.exe, or rundll32.exe — these represent T1059 sub-techniques (T1059.001, T1059.003, T1059.005) spawned from the Outlook process tree. Use the Sigma rule 'proc_creation_win_outlook_spawn_susp_process' (available in SigmaHQ repository) converted to Windows Event Log queries via sigma-cli. For Exchange, parse SMTP receive logs at '%ExchangeInstallPath%\TransportRoles\Logs\FrontEnd\SmtpReceive\' using PowerShell: 'Select-String -Path "*.log" -Pattern "Content-Type:.{0,200}(base64|uuencode|binhex)" | Where-Object {$_.Line -match "X-MS-Exchange"}' to identify anomalous encoding in pre-delivery messages.

Evidence: Capture Sysmon Event ID 1 logs showing OUTLOOK.EXE as ParentProcessId for any child process spawned during the exposure window; preserve the full command-line field. Collect Windows Security Event Log Event ID 4688 (Process Creation with command-line auditing enabled) filtering on processes where ParentProcessName = 'OUTLOOK.EXE'. Extract raw MIME source of any suspicious inbound messages from Exchange Recoverable Items or the transport dumpster at 'Get-MailboxFolderStatistics -Identity -FolderScope RecoverableItems' — the crafted email itself is primary forensic evidence for a zero-click exploit and must not be deleted. Preserve Exchange Message Tracking Logs at '%ExchangeInstallPath%\TransportRoles\Logs\MessageTracking\' for the relevant delivery window.

Step 3: Eradication — Apply the Microsoft patch released for CVE-2026-40361 via Windows Update, Microsoft Update Catalog, or your enterprise patch management platform. Specific KB article and patch ID should be confirmed directly from the MSRC advisory. For environments where patching is delayed, consider disabling automatic email preview rendering in Outlook as a temporary mitigation, and enforce email inspection at the gateway to strip or quarantine anomalous message structures.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), 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: Disable Outlook's automatic email preview rendering immediately as a compensating control: set the registry key 'HKCU:\Software\Microsoft\Office\\Outlook\Options\Mail' DWORD 'DisableAttachmentPreview' to 1, and enforce 'Plain Text' reading mode via GPO (User Configuration > Administrative Templates > Microsoft Outlook > Outlook Options > Preferences > Email Options: 'Read all standard mail in plain text'). For gateway-level mitigation without commercial sandboxing, configure Postfix or Exchange transport rules to reject or quarantine messages with MIME parts exceeding header size thresholds or containing malformed Content-Type declarations. Apply the specific KB from the MSRC advisory using 'wusa.exe /install /kb: /quiet /norestart' scripted via batch or PowerShell Invoke-Command across the estate.

Evidence: Before applying the patch, image or snapshot the memory of any Outlook process on systems suspected of compromise using ProcDump ('procdump.exe -ma OUTLOOK.EXE outlook_pre_patch.dmp') to preserve in-memory artifacts of potential shellcode or injected code that the zero-click exploit may have placed in the Outlook process heap. Capture the pre-patch Outlook binary version from 'OUTLOOK.EXE' file properties and hash it (Get-FileHash) for chain-of-custody documentation. Record the current state of the Outlook add-in registry keys at 'HKCU:\Software\Microsoft\Office\Outlook\Addins' and 'HKLM:\SOFTWARE\Microsoft\Office\Outlook\Addins' — a successful exploit may establish persistence via a malicious COM add-in.

Step 4: Recovery — After patching, verify patch installation via endpoint management console or registry key confirmation per MSRC guidance. Re-enable any email delivery restrictions applied as temporary containment. Monitor Outlook process behavior for 72 hours post-patch for residual anomalous activity. Confirm no lateral movement occurred on systems that were exposed and unpatched during the window between disclosure and patch application.

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 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify patch installation without enterprise tooling by querying 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages' for the specific KB package name or checking the ClickToRun version at 'HKLM:\SOFTWARE\Microsoft\Office\ClickToRun\Configuration' (VersionToReport) against the patched build number published in the MSRC advisory. For lateral movement verification, run 'net localgroup administrators' and review Windows Security Event ID 4728 (member added to global security group) and 4732 (member added to local group) on all hosts that ran unpatched Outlook, focusing on the exposure window. Use osquery 'SELECT * FROM logged_in_users' and 'SELECT * FROM process_open_sockets WHERE pid IN (SELECT pid FROM processes WHERE name = "OUTLOOK.EXE")' to detect residual network connections from Outlook that should not exist post-patch.

Evidence: Prior to re-enabling email flow, review Windows Security Event ID 4624 (Successful Logon) and 4648 (Logon with explicit credentials) on exposed hosts for logon types 3 (network) and 10 (remote interactive) during the exposure window, which would indicate credential use following a potential compromise via the zero-click exploit. Collect scheduled task artifacts via 'schtasks /query /fo CSV /v > scheduled_tasks_post_patch.csv' and compare against a known-good baseline — zero-click RCE exploits frequently establish persistence through scheduled tasks or WMI subscriptions. Preserve Windows prefetch files from 'C:\Windows\Prefetch\' for any executable invoked from the Outlook process tree during the exposure window.

Step 5: Post-Incident — Review your patch deployment SLA for critical Microsoft Office/Outlook CVEs and evaluate whether the time-to-patch target was met. Assess whether email security gateway controls (sandboxing, MIME inspection, attachment stripping) would have reduced exposure during the patch gap. Map control gaps to NIST SP 800-53 controls SI-2 (Flaw Remediation) and SI-3 (Malicious Code Protection). Consider adding zero-click Outlook exploitation to your threat hunting hypothesis backlog for future proactive hunts.

NIST Phase: Post Incident

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

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Formalize a threat hunting hypothesis specifically for zero-click Outlook exploitation using the MITRE ATT&CK Navigator to map T1566.001 (Spearphishing Attachment), T1203 (Exploitation for Client Execution), and T1059 sub-techniques as your detection chain. Author a Sigma rule targeting OUTLOOK.EXE spawning any process in the Windows scripting host family and submit it to your internal detection backlog. Conduct a tabletop exercise simulating zero-click email delivery to an unpatched Outlook host to measure actual detection time against your SLA; document gaps in a post-incident report mapped to NIST IR-8 (Incident Response Plan) requirements for plan updates.

Evidence: Preserve the complete Exchange message tracking log export covering the full exposure window as a permanent incident record per NIST AU-11 (Audit Record Retention). Document the delta between MSRC advisory publication timestamp and confirmed patch deployment across the estate — this metric directly measures your SI-2 (Flaw Remediation) control effectiveness. Retain all Sysmon and Windows Event Log exports from exposed hosts for a minimum of 12 months to support potential future forensic review if delayed-action malware or persistence mechanisms surface after the incident closure.

Detection Guidance

Primary behavioral indicator: OUTLOOK.EXE spawning unexpected child processes (cmd.exe, powershell.exe, wscript.exe, mshta.exe, or any scripting interpreter) without user-initiated action. Query EDR process tree logs filtering on parent process name OUTLOOK.EXE with child process category matching interpreters or network tools. Secondary indicator: Outlook generating outbound network connections to non-Microsoft destinations immediately following email receipt, prior to any user interaction event. At the email gateway, flag messages with malformed Content-Type headers, excessively nested MIME boundaries, or binary content in header fields; these patterns are consistent with CWE-122 heap overflow trigger payloads, though specific payload signatures are not confirmed at this time. No confirmed IOC hashes, IP addresses, or domains are available from current sources. Behavioral detection via EDR is the most reliable current approach. Cross-reference any detections with T1203 and T1059 ATT&CK technique telemetry in your SIEM.

Framework Mappings

MITRE-ATTACK

- **T1566.001** — Spearphishing Attachment
- **T1059** — Command and Scripting Interpreter
- **T1203** — Exploitation for Client Execution

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
	https://www.securityweek.com/microsoft-patches-critical-zero-click-...	T3
Microsoft Patches Zero-Click Outlook Vulnerability That Could Soon ...	https://www.securityweek.com/microsoft-patches-zero-click-outlook-v...	T3
Zero-Click Critical Microsoft Outlook Vulnerability. What You Need to ...	https://ironscales.com/blog/zero-click-critical-microsoft-outlook-v...	T3
Microsoft Patches Zero-Click Outlook Vulnerability That Could Soon ...	https://www.linkedin.com/pulse/microsoft-patches-zero-click-outlook...	T3
Patch Now: Microsoft Flags Zero-Day & Critical Zero-Click Bugs	https://www.darkreading.com/vulnerabilities-threats/patch-now-micro...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-40361	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361	T1

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-13 14:28 UTC by TJS Security Command Center