INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 06:33 UTC

Critical Privilege Escalation Vulnerabilities in Microsoft Exchange Online and Microsoft 365 Copilot (CVE-2026-54998, CVE-2026-41106)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0387
Type	CVE Vulnerability
CVE ID	CVE-2026-54998, CVE-2026-41106
Severity	CRITICAL
CVSS Base Score	9.1
EPSS Score	0.0064 (46th percentile)
Affected Products	Microsoft Exchange Online; Microsoft 365 Copilot
Published	2026-07-04
Discovery Source	Gemini

Executive Summary

Microsoft disclosed two critical privilege escalation vulnerabilities affecting Exchange Online (CVE-2026-54998) and Microsoft 365 Copilot (CVE-2026-41106), both patched server-side by Microsoft prior to public disclosure with no customer action required. CVE-2026-54998 stems from incorrect authorization logic; CVE-2026-41106 exploits an open redirect weakness in Copilot. Because remediation was applied before public disclosure, residual risk for most organizations is low, though exploitation during the pre-patch window cannot be ruled out based on available sources.

Technical Analysis

Two critical privilege escalation vulnerabilities were disclosed affecting Microsoft cloud services. CVE-2026-41106 (CWE-601: Open Redirect) affects Microsoft 365 Copilot; NVD, CVE.org, and Tenable records are present for this CVE. CVE-2026-54998 (CWE-285: Improper Authorization) affects Microsoft Exchange Online; authoritative advisory presence is confirmed via the Microsoft Security Response Center (MSRC) advisory, though independent NVD confirmation is not available from provided source data. CVSS base score is reported at 9.1 (critical). EPSS score is 0.644% at the 46th percentile, indicating low current exploitation probability. Both map to MITRE ATT&CK T1078 (Valid Accounts) and T1550 (Use Alternate Authentication Material), consistent with privilege escalation chains targeting cloud identity contexts. No CISA KEV listing as of

the configuration date. CWE-601 in Copilot could allow an attacker to redirect users to a controlled endpoint and leverage resulting tokens or session context for escalation. CWE-285 in Exchange Online could allow a lower-privileged principal to perform actions beyond their authorization boundary. Microsoft patched both vulnerabilities server-side; no customer-applied patch is required. Confidence in core technical details is medium, per source metadata; primary corroboration rests on a third-party aggregator (threat-modeling.com, T3) and an AI-assisted discovery report (Gemini). T1 source coverage is stronger for CVE-2026-41106 than for CVE-2026-54998.

Action Checklist

1. Step 1: Containment. No customer-side patch is required; Microsoft applied server-side remediation to both Exchange Online and Microsoft 365 Copilot. Confirm your tenant is current by reviewing the MSRC advisories at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54998 and https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41106. If your organization proxies or federates Exchange Online or Copilot traffic through on-premises infrastructure, verify those components have not introduced a re-exposure path.
2. Step 2: Detection. Review Azure AD / Entra ID sign-in logs and Exchange Online audit logs for anomalous privilege changes or unexpected role assignments occurring in the window prior to Microsoft's patch deployment. Per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs), query unified audit logs for operations such as 'Add member to role', 'Update user', or 'Consent to application' by accounts that should not hold elevated permissions. For CVE-2026-41106, inspect Copilot activity logs for redirect events or token requests originating from unexpected domains. MITRE T1078 detection: flag logins from service principals or delegated permissions outside established baselines.
3. Step 3: Eradication. Both vulnerabilities are server-side; no on-premises patch or configuration change is required for the vulnerabilities themselves. Per NIST SI-2 (Flaw Remediation), document the server-side fix in your vulnerability tracking record, noting that remediation was vendor-applied. If audit logs reveal any privilege changes or suspicious access during the pre-patch window, revoke affected sessions and rotate credentials for implicated accounts per D3-CRO (Credential Rotation).
4. Step 4: Recovery. Validate that no persistent privileged roles or application consents were granted during the exposure window. Review Exchange Online role assignments and Copilot app permissions against your approved baseline. Per NIST IR-5 (Incident Monitoring), document any anomalous findings and close the monitoring window once a clean 30-day lookback is confirmed. Re-enable any alerting rules that were temporarily suppressed.
5. Step 5: Post-Incident. Assess whether your organization has adequate logging coverage per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to have detected exploitation had it occurred. Review Entra ID Privileged Identity Management (PIM) configurations. Map control gaps to CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) and CIS 6.5 (Require MFA for Administrative Access). Document the incident in your risk register, noting the medium-confidence source quality and the absence of CISA KEV listing.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate to senior IR leadership and legal/privacy counsel immediately if Unified Audit Log review reveals any confirmed 'Add member to role', 'Consent to application', or Copilot OAuth redirect events during the pre-patch exposure window attributable to unauthorized principals, as these would indicate actual exploitation of CVE-2026-54998 or CVE-2026-41106 and may trigger breach notification obligations under GDPR, HIPAA, or state privacy laws if Exchange Online mailbox data or Copilot-processed sensitive content was accessible to the escalated privilege.
Recovery Notes	Verify recovery integrity by confirming Exchange Online role assignments and Copilot enterprise application permission grants match your pre-exposure approved baseline, with no net-new standing privileged assignments present. Maintain the 30-day enhanced monitoring window on Entra ID 'Add member to role' and 'Consent to application' audit operations, as persistence mechanisms introduced via CVE-2026-54998 incorrect authorization logic (such as a silently granted delegated permission) may not surface immediately. Close the incident record only after the 30-day clean lookback is confirmed and the risk register entry is reviewed by the risk owner.
Forensic Artifacts	Microsoft 365 Unified Audit Log entries for 'Add member to role', 'Update user', and 'Consent to application' operations within the Exchange Online and Entra ID workloads during the pre-patch exposure window — primary artifact for detecting CVE-2026-54998 incorrect authorization exploitation | Entra ID Sign-In Logs (AuditLogs/SignIns via MS Graph) for the Copilot service principal, specifically entries where the OAuth redirect URI does not match the tenant's registered Copilot application URIs — primary artifact for CVE-2026-41106 open redirect token harvesting | Exchange Online Management Role Assignment audit trail ('Get-ManagementRoleAssignment' timestamped export) capturing any role grants created during the exposure window by service principals or accounts not in the approved administrator baseline | OAuth2 Permission Grant export ('Get-AzureADOAuth2PermissionGrant') capturing delegated or application-level permission grants to unexpected client applications against Exchange Online or Copilot resource service principals, which would indicate persistence established via the CVE-2026-54998 authorization bypass | Microsoft Purview Compliance Portal CopilotInteraction workload logs filtered for 'AISystemPlugin' invocations or external domain references, identifying whether CVE-2026-41106 open redirect was used to exfiltrate tokens or route Copilot responses to attacker-controlled endpoints

Per-Action IR Details

Step 1: Containment — No customer-side patch is required; Microsoft applied server-side remediation to both Exchange Online and Microsoft 365 Copilot. Confirm your tenant is current by reviewing the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-54998 and the corresponding CVE-2026-41106 entry. If your organization proxies or federates Exchange Online or Copilot traffic through on-premises infrastructure, verify those components have not introduced a re-exposure path.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For tenants routing Exchange Online or Copilot through an on-premises hybrid connector or proxy, run 'Get-HybridMailflowDatacenterIPs' in Exchange Online PowerShell and cross-reference with your firewall egress rules to confirm no local component re-exposes the incorrect authorization path from CVE-2026-54998. For CVE-2026-41106, inspect your Entra ID enterprise application proxy configuration: 'Get-AzureADApplicationProxyApplication' (Azure AD PowerShell) to enumerate any apps fronting Copilot traffic that could reintroduce the open redirect.

Evidence: Before verifying or altering any hybrid connector or proxy configuration, export current Exchange Online transport rule state ('Get-TransportRule | Export-Clixml') and capture active Entra ID conditional access policy snapshots via Microsoft Graph ('GET /identity/conditionalAccess/policies') so baseline state is preserved prior to any configuration change. These exports document pre-remediation authorization posture relevant to the CVE-2026-54998 incorrect authorization mechanism.

Step 2: Detection — Review Azure AD / Entra ID sign-in logs and Exchange Online audit logs for anomalous privilege changes or unexpected role assignments occurring in the window prior to Microsoft's patch deployment. Per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs), query unified audit logs for operations such as 'Add member to role', 'Update user', or 'Consent to application' by accounts that should not hold elevated permissions. For CVE-2026-41106, inspect Copilot activity logs for redirect events or token requests originating from unexpected domains. MITRE T1078 detection: flag logins from service principals or delegated permissions outside established baselines.

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: Without a SIEM, query the Microsoft 365 Unified Audit Log directly via PowerShell: 'Search-UnifiedAuditLog -StartDate -EndDate -Operations "Add member to role","Update user","Consent to application" -ResultSize 5000 | Export-Csv auditlog_privesc.csv'. For CVE-2026-41106 open redirect abuse, filter Entra ID sign-in logs for token issuances where the resource is the Copilot service principal and the redirect URI does not match your approved list: 'Get-AzureADAuditSignInLogs | Where-Object { $_.ResourceDisplayName -like "*Copilot*" -and $_.Status.ErrorCode -eq 0 }'. Both commands are executable by a 2-person team with only the Microsoft 365 audit reader role.

Evidence: Capture the following volatile log state BEFORE any session revocation or credential rotation performed as a result of findings: (1) full Entra ID sign-in log export for the exposure window ('AuditLogs/SignIns' via MS Graph) preserving IPAddress, conditionalAccessStatus, and appDisplayName fields; (2) Exchange Online role group membership snapshot ('Get-RoleGroupMember -Identity "Organization Management"' and all privileged groups) timestamped at discovery; (3) Copilot activity log export from Microsoft Purview compliance portal filtered on 'CopilotInteraction' workload, specifically retaining any entries where 'AISystemPlugin' or external domain OAuth redirect URIs appear, as these represent artifacts specific to CVE-2026-41106 open redirect token harvesting.

Step 3: Eradication — Both vulnerabilities are server-side; no on-premises patch or configuration change is required for the vulnerabilities themselves. Per NIST SI-2 (Flaw Remediation), document the server-side fix in your vulnerability tracking record, noting that remediation was vendor-applied. If audit logs reveal any privilege changes or suspicious access during the pre-patch window, revoke affected sessions and rotate credentials for implicated accounts per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling)

Compensating: To revoke all active sessions for a suspected compromised account without Entra ID P2 licensing, execute: 'Revoke-AzureADUserAllRefreshToken -ObjectId ' followed by 'Set-AzureADUser -ObjectId -AccountEnabled $false' then re-enable after password reset. For any service principal that received unauthorized 'Consent to application' grants during the CVE-2026-54998 exposure window, remove the OAuth permission grant: 'Remove-AzureADOAuth2PermissionGrant -ObjectId '. Document each action with timestamp and actor in your vulnerability tracking record as the vendor-applied fix record.

Evidence: CRITICAL — volatile evidence must be captured BEFORE revoking sessions or rotating credentials: (1) export all current OAuth2 permission grants for the tenant ('Get-AzureADOAuth2PermissionGrant -All $true | Export-Csv oauth_grants_pre_revocation.csv') to document any unauthorized application consents that may have been introduced via CVE-2026-54998 incorrect authorization logic; (2) capture active refresh token sessions for

implicated accounts via MS Graph ('GET /users/{id}/authentication/signInActivity'); (3) screenshot or export any Exchange Online role assignments added during the exposure window ('Get-ManagementRoleAssignment | Where-Object { $_.WhenCreated -gt }') before revocation destroys the live assignment state.

Step 4: Recovery — Validate that no persistent privileged roles or application consents were granted during the exposure window. Review Exchange Online role assignments and Copilot app permissions against your approved baseline. Per NIST IR-5 (Incident Monitoring), document any anomalous findings and close the monitoring window once a clean 30-day lookback is confirmed. Re-enable any alerting rules that were temporarily suppressed.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-5 (Incident Monitoring), NIST IR-4 (Incident Handling), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without an IGA (Identity Governance and Administration) tool, validate Exchange Online role assignments against a previously exported baseline using PowerShell diff: 'Compare-Object (Import-Csv baseline_roles.csv) (Get-ManagementRoleAssignment | Select-Object Name,Role,RoleAssigneeName | Export-Csv current_roles.csv -PassThru) -Property RoleAssigneeName'. For Copilot app permissions, compare current enterprise application consent grants against your last known-good export. Schedule a recurring weekly 'Search-UnifiedAuditLog' job via Windows Task Scheduler for the 30-day monitoring window, filtering on 'Add member to role' and 'Consent to application' operations.

Evidence: Before closing the monitoring window, preserve: (1) a final Exchange Online management role assignment export as the post-recovery baseline; (2) the Copilot enterprise application permission grant state from MS Graph ('GET /servicePrincipals/{copilot_id}/appRoleAssignments') as the verified clean-state snapshot; (3) Entra ID Conditional Access policy export confirming no policies were modified or disabled during the exposure window. These records serve as the recovery verification artifact per NIST 800-61r3 §3.5 and anchor the 30-day clean lookback start date.

Step 5: Post-Incident — Assess whether your organization has adequate logging coverage per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to have detected exploitation had it occurred. Review Entra ID Privileged Identity Management (PIM) configurations. Map control gaps to CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) and CIS 6.5 (Require MFA for Administrative Access). Document the incident in your risk register, noting the medium-confidence source quality and the absence of CISA KEV listing.

NIST Phase: Post Incident

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), NIST IR-8 (Incident Response Plan), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: To assess logging gaps without a SIEM, run Microsoft's free 'Microsoft 365 Secure Score' assessment in the M365 admin portal and cross-reference the 'Ensure audit log search is enabled' and 'Ensure Microsoft 365 audit log search is enabled for all users' checks against your findings. For PIM gap analysis without Entra ID P2, manually enumerate standing privileged role memberships versus eligible-only assignments: 'Get-AzureADDirectoryRole | ForEach-Object { Get-AzureADDirectoryRoleMember -ObjectId $_.ObjectId }' and document all accounts with permanent (non-time-bound) Exchange or Copilot administrative roles as a PIM adoption gap specific to the CVE-2026-54998 privilege escalation attack surface.

Evidence: No live state alteration occurs in this phase; evidence preservation focus shifts to documentation: retain the full audit log query results from Steps 2–4, the pre/post role assignment exports, and the OAuth grant inventory as the evidentiary package supporting risk register entry. Document the specific M365 Unified Audit Log retention period configured for your tenant (default 90 days for E3, 1 year for E5) as a finding, since a longer pre-patch exposure window than your retention period would constitute an undetectable blind spot specific to the timing of CVE-2026-54998 and CVE-2026-41106 disclosure.

Detection Guidance

Because both vulnerabilities are fully remediated server-side, detection focus is retrospective: determine whether exploitation occurred before patching. Query the Microsoft Unified Audit Log (UAL) for Exchange Online and Copilot workloads for the period prior to Microsoft's patch deployment. Key event operations to review: 'Add member to role', 'Add delegated permission grant', 'Update application', 'Set-MailboxPermission', and 'Consent to application'. For CVE-2026-41106 (open redirect in Copilot, CWE-601), look for Copilot sign-in events or OAuth token issuances referencing external redirect URIs not in your approved application registration list. For CVE-2026-54998 (improper authorization in Exchange Online, CWE-285), look for permission or role changes executed by accounts without a corresponding change-management record. MITRE T1078 behavioral indicator: service accounts or low-privilege users appearing in audit logs with elevated Exchange or M365 role assignments. MITRE T1550 behavioral indicator: token-based authentication events from unexpected client IDs or user agents against Exchange Online endpoints. Per NIST SI-4 and CIS 8.2, ensure UAL retention covers the full pre-patch window. D3-LAM (Local Account Monitoring) and D3-UAP (User Account Permissions) apply as retrospective review techniques.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1550** — Use Alternate Authentication Material

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SR-2** — Supply Chain Risk Management Plan

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1550	Use Alternate Authentication Material	Defense-Evasion

Sources

Source	URL	Tier
gemini	https://threat-modeling.com/vulnerability-intelligence-report-july-...	T3
CVE-2026-41106 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-41106	T1
Microsoft Exchange Online and 365 Copilot Critical ...	https://threat-modeling.com/cve-2026-54998-cve-2026-41106-exchange-...	T3
CVE Record: CVE-2026-41106	https://www.cve.org/CVERecord?id=CVE-2026-41106	T1
CVE-2026-41106	https://www.tenable.com/cve/CVE-2026-41106	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5499...	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-07-06 06:33 UTC by TJS Security Command Center