INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:20 UTC

CVE-2026-42824: One-Click Microsoft 365 Copilot Chain Enables Silent Data Exfiltration via Trusted URLs

CVE VULNERABILITY | CRITICAL | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0305
Type	CVE Vulnerability
CVE ID	CVE-2026-42824, CVE-2025-32711
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0050 (39th percentile)
Affected Products	Microsoft 365 Copilot Enterprise Search, Microsoft 365, Bing Search by Image endpoint
Published	2026-06-15T11:09:05
Discovery Source	Rss

Executive Summary

Varonis Threat Labs disclosed CVE-2026-42824, a critical chained vulnerability in Microsoft 365 Copilot Enterprise Search that allows an attacker to silently exfiltrate emails, calendar entries, SharePoint and OneDrive files, and live MFA codes with a single user click on a legitimate-appearing microsoft.com URL. The attack requires no malware, no elevated privileges, and bypasses AI guardrails by exploiting a trusted Bing endpoint to tunnel data past Content Security Policy controls. Microsoft has deployed a server-side mitigation; no tenant action is required, but security teams should validate exposure and monitor for similar AI-pipeline attack patterns.

Technical Analysis

CVE-2026-42824 is a chained attack against Microsoft 365 Copilot Enterprise Search rated CVSS 9.5 (Critical), disclosed by Varonis Threat Labs. The chain combines three weaknesses: (1) CWE-77 parameter-to-prompt injection, where attacker-controlled input manipulates Copilot's LLM prompt context without privilege escalation; (2) CWE-362 sanitizer race condition, allowing malicious content to pass input validation before guardrails engage; and (3) CWE-184/CWE-1021 Content Security Policy bypass exploiting Bing's Search by Image endpoint, a trusted microsoft.com/bing.com origin, to tunnel exfiltrated data past CSP allow-lists. Data at risk includes email content, calendar data, indexed SharePoint/OneDrive files, and live MFA codes. The attack fires

on a single victim click, requires no malware deployment, and is pre-guardrail. MITRE techniques mapped include T1048.003 (exfiltration over alternative protocol), T1114.002 (remote email collection), T1530 (data from cloud storage), T1566.001 (phishing: spearphishing link), and T1190 (exploit public-facing application). Related CVE-2025-32711 ('EchoLeak') is a zero-click variant in the same AI-pipeline attack class. Microsoft applied a server-side fix; no tenant-side patch or configuration change is required. EPSS score is 0.00503 (38th percentile); CISA KEV listing has not been confirmed as of the configuration date.

Action Checklist

1. Step 1: Containment, Confirm your tenant is covered by Microsoft's server-side mitigation by reviewing the Microsoft Security Response Center advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42824. Because the fix is server-side, no tenant patch action is required; however, verify that Microsoft 365 Copilot Enterprise Search is not configured with custom connector permissions that could expand the blast radius of any residual prompt-injection path.
2. Step 2: Detection, Query Microsoft 365 Unified Audit Logs (UAL) for anomalous Copilot activity: look for high-volume search queries, unexpected cross-workload data access (mail + calendar + SharePoint in a single session), and outbound requests to Bing Search by Image endpoints (bing.com/images/search) originating from Copilot service principals. Review Azure AD sign-in logs for MFA code reuse or rapid successive authentications following Copilot sessions. Alert on T1114.002 and T1530 behavioral patterns in your SIEM.
3. Step 3: Eradication, No tenant-side patch exists; the mitigation is fully server-side per Microsoft. Reduce residual attack surface by scoping Copilot Enterprise Search permissions to least-privilege data sources (NIST AC-6), disabling Copilot access to mailbox and calendar data for roles that do not require it, and reviewing and tightening SharePoint/OneDrive sharing policies to limit what Copilot can index and return.
4. Step 4: Recovery, After confirming Microsoft's server-side fix is active, validate that no exfiltration events occurred during the exposure window by auditing UAL for the indicators described in Step 2. Rotate credentials for any accounts that accessed Copilot Enterprise Search between initial disclosure and confirmed mitigation. Confirm MFA codes are not being replayed in Azure AD logs. Restore any modified Copilot connector configurations to documented baselines.
5. Step 5: Post-Incident, Review AI-integrated application permissions enterprise-wide; prompt-injection/CSP-bypass chains are now an established attack class for AI productivity platforms (see also CVE-2025-32711 EchoLeak). Map control gaps to NIST AC-4 (information flow enforcement between Copilot and connected data stores), NIST SI-4 equivalent monitoring for AI pipeline activity, and CIS 6.3 (require MFA for externally-exposed applications). Develop a standing detection rule for outbound Bing image-search endpoint calls from M365 service principals. Brief your GRC team on AI-pipeline attack patterns for inclusion in the next risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and your Data Protection Officer immediately if UAL analysis confirms that any Copilot session during the exposure window accessed mailboxes or SharePoint sites containing regulated data (PII, PHI, financial records, or legal privileged material), or if Azure AD logs show MFA codes captured via the exfiltration chain were subsequently used to authenticate from an unrecognized IP or device, as either condition may trigger mandatory breach notification obligations under GDPR, HIPAA, or applicable state privacy laws.
Recovery Notes	After Microsoft confirms server-side mitigation is active for your tenant, conduct a full UAL sweep covering the period from CVE-2026-42824 disclosure to confirmed fix deployment, specifically hunting for the tri-workload Copilot session pattern (Exchange + SharePoint + Calendar in a single session) combined with same-session Bing authentication events, which is the composite forensic signature of successful exploitation. Any accounts matching this pattern should be treated as potentially compromised — rotate credentials, revoke all active sessions via `Revoke-MgUserSignInSession`, and review Entra ID for unauthorized MFA method registrations before restoring those accounts to production use. Maintain elevated UAL monitoring for Copilot service principal activity and Bing endpoint authentication anomalies for a minimum of 30 days post-remediation, as prompt-injection/CSP-bypass chains in AI platforms have demonstrated delayed second-stage exploitation in related campaigns including CVE-2025-32711.
Forensic Artifacts	Microsoft 365 Unified Audit Log (UAL) CopilotInteraction records: filter on `RecordType eq 'CopilotInteraction'` for sessions where a single user identity accessed Exchange (`MailItemsAccessed`), SharePoint (`FileAccessed`), and Calendar workloads within the same session window — this tri-workload concurrent access pattern is the primary forensic indicator of CVE-2026-42824 exploitation and distinguishes it from normal Copilot usage. | Azure AD / Microsoft Entra ID sign-in logs for the Bing Search service principal: query for authentication events where the authenticating identity is a Copilot service account or where the Bing authentication timestamp falls within 60 seconds of a CopilotInteraction UAL event for the same user — this correlation maps the CSP-bypass exfiltration tunnel from the Copilot pipeline to the `bing.com/images/search` endpoint. | Microsoft Entra ID audit logs for MFA method registration events (`Add MFA method`, `User registered security info`) occurring during or immediately after Copilot sessions in the exposure window — the CVE-2026-42824 chain can exfiltrate live MFA codes, enabling an attacker to register a persistent authenticator and achieve durable account access. | SharePoint and OneDrive access logs (Purview audit `FileAccessed` and `SearchQueryInitiatedSharePoint` records): filter for queries returning anomalously high document counts or accessing sensitive-labeled sites within Copilot sessions — identifies what data was in scope for exfiltration and supports regulated-data breach notification analysis. | Microsoft Entra ID Conditional Access and Identity Protection risky sign-in reports: export risk events flagged for accounts that had Copilot sessions during the exposure window, specifically looking for token replay, impossible travel, or unfamiliar sign-in properties following the Copilot session — confirms whether captured session tokens or MFA codes were used for follow-on unauthorized access.

Per-Action IR Details

Step 1: Containment — Confirm your tenant is covered by Microsoft's server-side mitigation by reviewing the Microsoft Security Response Center advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42824. Because the fix is server-side, no tenant patch action is required; however, verify that Microsoft 365 Copilot Enterprise Search is not configured with custom connector permissions that could expand the blast radius of any residual prompt-injection path.

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without a vendor portal, query the Microsoft Graph API using PowerShell (`Get-MgServicePrincipal -Filter "displayName eq 'Microsoft Copilot'"`) to enumerate Copilot service principal delegated permissions. Manually audit custom connector OAuth scopes in the Microsoft 365 Admin Center under Settings > Integrated Apps. Document every delegated permission against the principle of least privilege before any scope reduction.

Evidence: Before modifying any Copilot connector configurations, capture a timestamped export of the current Copilot service principal permission grants via `Get-MgOauth2PermissionGrant` (Microsoft Graph PowerShell) and a full export of Copilot Enterprise Search connector configurations from the Microsoft 365 Admin Center. Export the Microsoft 365 Unified Audit Log (UAL) filtered to Copilot operations (`RecordType eq 'CopilotInteraction'`) for the window between CVE-2026-42824 disclosure and confirmed server-side mitigation — this volatile snapshot establishes your exposure baseline before configuration changes obscure it.

Step 2: Detection — Query Microsoft 365 Unified Audit Logs (UAL) for anomalous Copilot activity: look for high-volume search queries, unexpected cross-workload data access (mail + calendar + SharePoint in a single session), and outbound requests to Bing Search by Image endpoints (bing.com/images/search) originating from Copilot service principals. Review Azure AD sign-in logs for MFA code reuse or rapid successive authentications following Copilot sessions. Alert on T1114.002 and T1530 behavioral patterns in your SIEM.

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), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell and the Microsoft 365 Management Activity API directly. Run: `Search-UnifiedAuditLog -StartDate -EndDate -RecordType CopilotInteraction -ResultSize 5000 | Where-Object { $_.Operations -match 'SearchQueryInitiatedSharePoint|SearchQueryInitiatedExchange' }` to surface cross-workload Copilot searches. For the Bing exfiltration tunnel, query Azure AD sign-in logs via Graph: `Get-MgAuditLogSignIn -Filter "appDisplayName eq 'Bing'" -Top 500` and correlate timestamps within 60 seconds of Copilot session events. Flag any account that triggered both a Copilot cross-workload query and a Bing authentication in the same session window.

Evidence: Primary: Microsoft 365 UAL CopilotInteraction records showing concurrent access to Exchange (`MailItemsAccessed`), SharePoint (`FileAccessed`), and Calendar workloads within a single session token — this tri-workload pattern is the forensic signature of the CVE-2026-42824 chain. Secondary: Azure AD sign-in logs for the Bing Search service principal showing authentications from Copilot service account identities correlated to user sessions. Tertiary: Microsoft Purview audit records for `SearchQueryInitiatedSharePoint` and `SearchQueryInitiatedExchange` events with anomalously high result counts or data volumes. Preserve all UAL records in immutable storage (e.g., export to Azure Blob with WORM policy) before any remediation action alters the audit trail.

Step 3: Eradication — No tenant-side patch exists; the mitigation is fully server-side per Microsoft. Reduce residual attack surface by scoping Copilot Enterprise Search permissions to least-privilege data sources (NIST AC-6), disabling Copilot access to mailbox and calendar data for roles that do not require it, and reviewing and tightening SharePoint/OneDrive sharing policies to limit what Copilot can index and return.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 3.3 (Configure Data Access Control Lists), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use the Microsoft 365 Admin Center (no-cost, tenant-included) to restrict Copilot Enterprise Search data sources: navigate to Settings > Search & Intelligence > Connectors and disable Mail and Calendar connectors for non-essential role groups. Use SharePoint Admin Center > Policies > Sharing to set tenant-wide external sharing to 'Only people in your organization' as a temporary hardening measure. Script a bulk review of Sensitivity Labels applied to SharePoint sites that Copilot can index using: `Get-SPOSite -Limit All | Select Url,SharingCapability,ConditionalAccessPolicy` (requires SharePoint Online Management Shell).

Evidence: Before disabling any Copilot connector or revoking mailbox/calendar access, capture: (1) a full export of active Copilot connector configurations and their OAuth permission scopes; (2) current SharePoint site sensitivity label and sharing policy states via `Get-SPOSite` export; (3) a final UAL pull for `CopilotInteraction` records up to the moment of permission change — any exfiltration events that occurred between initial exposure and this eradication step will not appear in post-change logs. These captures constitute the forensic record of the maximum exposure window for regulatory breach notification purposes.

Step 4: Recovery — After confirming Microsoft's server-side fix is active, validate that no exfiltration events occurred during the exposure window by auditing UAL for the indicators described in Step 2. Rotate credentials for any accounts that accessed Copilot Enterprise Search between initial disclosure and confirmed mitigation. Confirm MFA codes are not being replayed in Azure AD logs. Restore any modified Copilot connector configurations to documented baselines.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), NIST AU-9 (Protection of Audit Information), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation without automated provisioning tooling, prioritize accounts by Copilot session volume from the UAL export: accounts with the highest cross-workload query counts are highest-risk for credential compromise via MFA code exfiltration. Use the Azure AD Portal to force password reset and revoke all refresh tokens simultaneously via: `Revoke-MgUserSignInSession -UserId ` (Microsoft Graph PowerShell) — this invalidates any session tokens that may have been captured during the attack chain. Monitor Azure AD risky sign-in reports (Identity Protection) for 30 days post-rotation for replay attempts.

Evidence: Before rotating credentials or revoking sessions for any account, capture: (1) Azure AD sign-in log export for each target account covering the full exposure window, with specific attention to authentication events from IP addresses or user agents inconsistent with the account's normal pattern following Copilot sessions; (2) Microsoft Entra ID audit logs for any MFA method registrations or changes that occurred during the exposure window — an attacker who captured live MFA codes via the CVE-2026-42824 chain may have used them to register a persistent authentication method; (3) UAL records for `Add MFA method` and `User registered security info` operations. Session revocation destroys the live token state that could otherwise confirm active attacker persistence.

Step 5: Post-Incident — Review AI-integrated application permissions enterprise-wide; prompt-injection/CSP-bypass chains are now an established attack class for AI productivity platforms (see also CVE-2025-32711 EchoLeak). Map control gaps to NIST AC-4 (information flow enforcement between Copilot and connected data stores), NIST SI-4 equivalent monitoring for AI pipeline activity, and CIS 6.3 (require MFA for externally-exposed applications). Develop a standing detection rule for outbound Bing image-search endpoint calls from M365 service principals. Brief your GRC team on AI-pipeline attack patterns for inclusion in the next risk assessment cycle.

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-13 (Monitoring for Information Disclosure), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Develop a standing Sigma rule targeting UAL CopilotInteraction records where a single session references three or more distinct workload types (Exchange + SharePoint + Calendar) within a 5-minute window,

correlated with a subsequent Bing authentication event from the same identity — this composite pattern is the behavioral signature of both CVE-2026-42824 and structurally similar prompt-injection/CSP-bypass chains like CVE-2025-32711. Store the rule in a version-controlled repository (Git) as the foundation of your AI-pipeline detection program. Use Microsoft Secure Score in the Microsoft 365 Defender portal (no additional cost) to track MFA enforcement gaps for CIS 6.3 compliance across all Copilot-licensed accounts.

Evidence: The post-incident evidence package for the GRC brief and risk assessment should include: (1) preserved UAL export covering the full CVE-2026-42824 exposure window, retained per your audit record retention policy (NIST AU-11); (2) a documented inventory of all AI-integrated applications (Copilot, Power Automate connectors, third-party Graph API apps) and their delegated permission scopes as of incident closure — this becomes the baseline for future AI-pipeline risk assessments; (3) Microsoft Entra ID conditional access policy export showing MFA enforcement state at time of incident, to support breach notification analysis if regulated data (PII, HIPAA-covered PHI, financial records) was accessible to Copilot during the exposure window.

Detection Guidance

Primary log source: Microsoft 365 Unified Audit Log (UAL), Operations: 'CopilotInteraction', 'SearchQueryPerformed', 'FileAccessed', 'MailItemsAccessed'. Secondary: Azure AD sign-in logs for MFA anomalies post-Copilot session. Behavioral indicators: (1) A single user session triggering cross-workload reads spanning Exchange mailbox, calendar, and SharePoint/OneDrive within a short time window, atypical for normal Copilot use. (2) Outbound HTTP requests from M365 service principals to bing.com/images/search or equivalent Bing Search by Image endpoints, particularly with URL-encoded query parameters carrying encoded data strings. (3) MFA code issuance events (OATH TOTP or SMS) immediately followed by rapid successive authentication attempts from new IP addresses. (4) Copilot search queries containing prompt-injection markers: unusual delimiters, role-override tokens, or instruction strings embedded in document content retrieved by Copilot. MITRE alignment: T1048.003 (watch for data tunneled in image search query parameters), T1114.002 (unexpected bulk mail read operations via Copilot service principal), T1530 (anomalous SharePoint/OneDrive file enumeration within Copilot context), T1566.001 (monitor for crafted microsoft.com URLs delivered via email or Teams). No public IOC hashes or IP indicators have been published as of this disclosure; detection is behavioral. Correlated framework controls: NIST AU-6 (audit record review for anomalous patterns), NIST AU-12 (audit record generation across M365 workloads), CIS 8.2 (collect audit logs across enterprise assets).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`bing.com/images/search (with anomalous encoded query parameters from M365 service principals)`	Bing Search by Image endpoint exploited as trusted CSP-allowed origin to tunnel exfiltrated data; legitimate endpoint repurposed as exfiltration channel — look for calls from Copilot service contexts with base64 or percent-encoded data in query strings	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1048.003** — Exfiltration Over Unencrypted Non-C2 Protocol

- **T1114.002** — Remote Email Collection
- **T1071.001** — Web Protocols
- **T1530** — Data from Cloud Storage
- **T1059** — Command and Scripting Interpreter
- **T1185** — Browser Session Hijacking
- **T1190** — Exploit Public-Facing Application
- **T1557** — Adversary-in-the-Middle
- **T1566.002** — Spearphishing Link
- **T1566** — Phishing
- **T1114** — Email Collection

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection

OWASP-TOP10-2021

- **A10:2021** — Server-Side Request Forgery (SSRF)
- **A03:2021** — Injection

CIS-V8

- **13.4** — Perform Traffic Filtering Between Network Segments
- **16.10** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1048.003	Exfiltration Over Unencrypted Non-C2 Protocol	Exfiltration
T1114.002	Remote Email Collection	Collection
T1071.001	Web Protocols	Command-And-Control
T1530	Data from Cloud Storage	Collection
T1059	Command and Scripting Interpreter	Execution
T1185	Browser Session Hijacking	Collection
T1190	Exploit Public-Facing Application	Initial-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1566.002	Spearphishing Link	Initial-Access
T1566	Phishing	Initial-Access
T1114	Email Collection	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/one-click-microsoft-365-copilot-f...	T3
CVE-2025-32711 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-32711	T1
CVE-2025-32711 Vulnerability: “EchoLeak” Flaw in Microsoft 365 ...	https://socprime.com/blog/cve-2025-32711-zero-click-ai-vulnerability/	T3
CVE-2025-32711 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2025-32711	T3
Security Update Guide - Microsoft Security Response Center	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42824	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-42824, CVE-2025-32711	T1

Source	URL	Tier
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-4282...	**T1**

Generated 2026-06-16 07:20 UTC by TJS Security Command Center