INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:35 UTC

Zero-Click Microsoft Excel Vulnerability Enables Copilot-Assisted Data Exfiltration

CVE VULNERABILITY | HIGH | CVSS 8.6

SCC Item ID	SCC-CVE-2026-0013
Type	CVE Vulnerability
CVE ID	CVE-2026-0013
Severity	HIGH
CVSS Base Score	8.6
Affected Products	Microsoft Excel (with Copilot integration); specific version ranges not confirmed in available sources
Published	2026-03-12

Executive Summary

A reported vulnerability in Microsoft Excel allows attackers to exfiltrate sensitive data by weaponizing Excel's Copilot integration when a malicious spreadsheet file is opened; no user interaction within Excel is required beyond opening the file. Organizations using Microsoft 365 with Copilot enabled in Excel may be potentially exposed to silent data theft from spreadsheets containing confidential business, financial, or personnel data. **CRITICAL: As of 2026-03-11, this vulnerability has not been officially confirmed by Microsoft, listed in NIST NVD, or assigned a CVE identifier. The information below is sourced from technology news outlets and has not been independently verified against official vendor advisories.** Organizations should monitor the Microsoft Security Response Center (https://msrc.microsoft.com) for official confirmation before operational escalation. Treat this as a preliminary alert pending verification.

Technical Analysis

An unconfirmed information disclosure vulnerability affecting Microsoft Excel with Copilot integration has been reported by multiple technology news outlets (The Register, Forbes, TechRadar, PCPer) as of 2026-03-11. **No official Microsoft Security Response Center advisory, CVE assignment, or vendor confirmation has been located.** The following description is based on tech press reporting and has not been independently verified against official sources. The reported attack vector involves a crafted spreadsheet that silently invokes Excel's Copilot agent functionality upon file open, reading and transmitting spreadsheet contents without user interaction within the Excel interface. Relevant CWEs are CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-862 (Missing Authorization). MITRE ATT&CK technique coverage includes

T1530 (Data from Cloud Storage), T1566.001 (Spearphishing Attachment), T1005 (Data from Local System), and T1041 (Exfiltration Over C2 Channel). A CVSS base score of 8.6 (High) has been reported in tech press, but the official CVSS vector string is not available, and the score has not been published by NIST or Microsoft. Specific affected build numbers, full exploitation mechanism, patch availability, and an official Microsoft advisory have not been confirmed from available sources. Affected version scope stated as Microsoft Excel with Copilot integration; specific build ranges require verification against a Microsoft Security Response Center advisory. EPSS score and KEV listing are not available at this time. Organizations should monitor MSRC (https://msrc.microsoft.com) and NVD (https://nvd.nist.gov) for official confirmation before operational decisions.

Action Checklist

1. Step 1, Immediate: Verify official status, Monitor the Microsoft Security Response Center (https://msrc.microsoft.com) and NIST NVD (https://nvd.nist.gov) for an official advisory and CVE assignment. This item is based on unconfirmed tech press reports as of 2026-03-11.
2. Step 2a, Immediate (if unconfirmed): Monitor Copilot integration settings in Microsoft 365 admin center and review current access permissions. Do not restrict functionality pending official confirmation.
3. Step 2b, If Confirmed by Microsoft: Once an official MSRC advisory is published, evaluate whether disabling or restricting Excel Copilot agent functionality is warranted based on Microsoft's mitigation guidance and your risk tolerance.
4. Step 3, Awareness: Review Microsoft 365 audit logs and Copilot activity logs for unexpected data access or outbound data transfer events originating from Excel sessions. Implement as awareness-level monitoring only until official confirmation.
5. Step 4, Assessment: Inventory Microsoft 365 users with Copilot licenses and Excel access to sensitive data repositories; prioritize monitoring for users who receive external spreadsheet files via email or collaboration platforms.
6. Step 5, Communication: Notify relevant business units and data owners of the preliminary report; advise caution with Excel files from untrusted sources. Escalate to formal security advisory only upon official Microsoft confirmation.
7. Step 6, Long-term: Once this vulnerability is officially confirmed or dismissed by Microsoft, review Microsoft 365 Copilot data access permissions and least-privilege controls; evaluate whether Copilot agent capabilities require explicit scope restrictions aligned with your data classification policy.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal/compliance immediately if Microsoft issues an MSRC advisory confirming active exploitation or widespread exposure; escalate to external IR firm if forensic evidence indicates successful exfiltration from your organization or if Copilot activity logs show suspicious data access patterns prior to official confirmation.

Recovery Notes	Post-incident recovery depends on confirmation status. If confirmed: restore Copilot access only after Microsoft releases a security update; implement granular conditional access policies to restrict Copilot scopes by data classification; conduct a 30-day forensic review of audit logs to detect silent exfiltration during the vulnerability window. If dismissed: restore full Copilot functionality and schedule a post-incident review to identify detection blind spots and communication delays in future unconfirmed threat handling.
Forensic Artifacts	Microsoft 365 Unified Audit Log (ExchangeAdmin, SharePoint, MicrosoftTeams record types, filtered for Copilot API calls and Excel file access; 90-day retention default) | Azure AD sign-in logs (filtered for Copilot service principal and user sessions; 30-day retention, or longer if Advanced Audit enabled) | Microsoft 365 admin center activity reports (Office 365 usage reports; app launches and service calls) | Windows Event Logs on affected machines: Security 4688 (process creation for msexcel.exe and copilot.exe processes), System (service start/stop events), and Application logs (any Copilot agent errors or data transfer alerts) | Network traffic captures (PCAP) from endpoints: filter for HTTPS POST requests to api.copilot.microsoft.com or graph.microsoft.com with Excel-related payloads; preserve TLS handshakes for certificate chain validation

Per-Action IR Details

Step 1, Immediate: Verify official status, Monitor the Microsoft Security Response Center (https://msrc.microsoft.com) and NIST NVD (https://nvd.nist.gov) for an official advisory and CVE assignment. This item is based on unconfirmed tech press reports as of 2026-03-11.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: threat intelligence and vulnerability monitoring)

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 4.1 (Vulnerability Management Program)

Compensating: Subscribe to Microsoft Security Update Guide RSS feed (https://www.microsoft.com/en-us/msrc/rss) and cross-reference against NVD weekly. Assign one person to check MSRC every Monday morning; document findings in a shared spreadsheet with date, status (unconfirmed/confirmed), and action decision.

Evidence: Capture the date and time you first received the threat report; document the source (e.g., vendor alert, news outlet, internal SOC). Screenshot the current MSRC and NVD pages as baseline. Store URLs and timestamps in your change log to establish when official confirmation (or dismissal) occurred.

Step 2a, Immediate (if unconfirmed): Monitor Copilot integration settings in Microsoft 365 admin center and review current access permissions. Do not restrict functionality pending official confirmation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (advance preparation: inventory and access control baseline); NIST 800-53r5 AC-2 (Account Management)

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 6.2 (Application Allow and Deny Lists)

Compensating: Use Microsoft 365 admin center (no cost) to export Copilot license assignments via PowerShell: Get-MsolUser -All | Where-Object {$_.Licenses -match 'Copilot'} | Export-Csv copilot_users.csv. Review Excel app permissions in Azure AD: Security > Enterprise Applications > Microsoft Excel > Permissions. Document current state in a baseline file for change detection.

Evidence: Export Copilot license roster before any changes (baseline). Capture screenshots of current Copilot permission scope in Azure AD and Microsoft 365 admin center. Document who has Copilot enabled and which data repositories they access (SharePoint sites, OneDrive folders). Preserve the date/time of this inventory.

Step 2b, If Confirmed by Microsoft: Once an official MSRC advisory is published, evaluate whether disabling or restricting Excel Copilot agent functionality is warranted based on Microsoft's mitigation guidance and your risk tolerance.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2 (containment phase: stopping the attack); NIST 800-53r5 IR-4 (Incident Handling)

Controls: NIST IR-4 (Incident Handling), NIST AC-3 (Access Enforcement), CIS 6.2 (Application Allow and Deny Lists)

Compensating: Disable Copilot for Excel tenant-wide via Microsoft 365 admin center (Settings > Services & add-ins > Microsoft Copilot) or use conditional access policies to restrict Copilot to non-sensitive data classifications. For teams without conditional access: manually disable Copilot licenses in bulk (PowerShell: Set-MsolUserLicense -UserPrincipalName user@domain.com -RemoveLicenses 'copilot_sku'). Implement daily change audits via Get-MsolAccountSku to detect any re-enabling.

Evidence: Before disabling Copilot, capture a snapshot of all Excel-to-Copilot API calls from the last 30 days (if available in Microsoft 365 audit logs: Search-UnifiedAuditLog -RecordType MicrosoftTeams -Operations '*Copilot*' -StartDate (Get-Date).AddDays(-30)). Document the date/time of the official MSRC advisory and your containment decision. Preserve the baseline license state for forensic comparison.

Step 3, Awareness: Review Microsoft 365 audit logs and Copilot activity logs for unexpected data access or outbound data transfer events originating from Excel sessions. Implement as awareness-level monitoring only until official confirmation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (detection and analysis: monitoring and investigation); NIST 800-53r5 AU-2 (Audit Events)

Controls: NIST AU-2 (Audit Events), NIST AU-6 (Audit Review, Analysis, and Reporting), CIS 8.2 (Collect and Analyze Logs)

Compensating: Use Microsoft 365 Security & Compliance Center (free): Search-UnifiedAuditLog -RecordType ExchangeAdmin -Operations 'Set-Mailbox' -StartDate (Get-Date).AddDays(-7) to find data access changes. For Copilot-specific activity: Search-UnifiedAuditLog -RecordType MicrosoftTeams -UserIds '*' -Operations '*Copilot*' -StartDate (Get-Date).AddDays(-7). Export to CSV and filter for 'External' or 'Shared' action types. Run weekly and store results in a change register.

Evidence: Preserve 30+ days of Microsoft 365 unified audit logs focusing on ExchangeAdmin, SharePoint, and MicrosoftTeams record types. Export baseline audit logs before any functional changes (Search-UnifiedAuditLog with -StartDate = 30 days ago; -EndDate = today). Identify and tag any records showing Excel file access + Copilot agent interaction in the same session. Note IP addresses, session IDs, and user agents.

Step 4, Assessment: Inventory Microsoft 365 users with Copilot licenses and Excel access to sensitive data repositories; prioritize monitoring for users who receive external spreadsheet files via email or collaboration platforms.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation: asset inventory and classification); NIST 800-53r5 IA-4 (Identifier Management)

Controls: NIST IA-4 (Identifier Management), NIST AC-2 (Account Management), CIS 2.1 (Inventory of Authorized Assets)

Compensating: Run PowerShell audit: Get-MsolUser -All | Where-Object {$_.Licenses -match 'COPILOT'} | Select-Object UserPrincipalName, DisplayName | Export-Csv copilot_users.csv. Cross-reference against SharePoint/OneDrive sensitivity labels: Get-SPOSite -Template 'TEAMCHANNEL#*' | Get-SPOList | Get-SPOListItem | Where-Object {$_['Sensitivity'] -match 'Confidential|Restricted'} to find Copilot users with classified data access. Manually review email rules for external file receipt patterns: Get-InboxRule | Where-Object {$_.BodyContainsWords -match '*.xlsx|*.xls'}.

Evidence: Export and date-stamp the Copilot license roster (baseline). Capture the list of sensitive SharePoint sites and their member lists. Document external email domains from which users receive spreadsheet attachments (parse email flow logs: Get-MessageTrace -StartDate (Get-Date).AddDays(-30) -SenderAddress '*@external.com' -Subject '*xlsx'). Establish a risk matrix: Copilot user + sensitive data access + frequent external file receipt = highest priority.

Step 5, Communication: Notify relevant business units and data owners of the preliminary report; advise caution with Excel files from untrusted sources. Escalate to formal security advisory only upon official Microsoft confirmation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (mitigation strategies and incident handling communication); NIST 800-53r5 IR-4 (Incident Handling), CP-4 (Contingency Plan Testing)

Controls: NIST IR-4 (Incident Handling), NIST CP-4 (Contingency Plan Testing), CIS 5.1 (Security Awareness and Training Program)

Compensating: Draft a preliminary security awareness message (email or Teams notification) from CISO/Security Lead stating: 'Unconfirmed report of Excel/Copilot data risk; do not open Excel files from untrusted external senders until further notice.' Post to internal wiki/intranet. Schedule a brief town hall or department briefing with IT, finance, HR (high-risk data owners). Document attendance and message delivery date. Escalate internally only; do not issue formal external advisory until MSRC confirmation.

Evidence: Preserve the date/time the preliminary report was issued internally. Document the distribution list (departments, data owners notified). Capture any incident reports or user questions triggered by the awareness message. If a user opens a suspicious Excel file before official confirmation, log the timestamp and user ID for retrospective forensics.

Step 6, Long-term: Once this vulnerability is officially confirmed or dismissed by Microsoft, review Microsoft 365 Copilot data access permissions and least-privilege controls; evaluate whether Copilot agent capabilities require explicit scope restrictions aligned with your data classification policy.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (post-incident activities: lessons learned); NIST 800-53r5 AC-3 (Access Enforcement), SI-12 (Information Management)

Controls: NIST AC-3 (Access Enforcement), NIST SI-12 (Information Management and Information Sharing), CIS 6.5 (Access Control Lists)

Compensating: Post-incident: audit Copilot scopes in Azure AD (Conditional Access policies) to restrict Copilot agents' read/write access to SharePoint sites, OneDrive folders, and Exchange mailboxes based on sensitivity labels (do not grant 'All Sites' or 'All Users' permissions). Document approved Copilot use cases (e.g., Copilot allowed for non-confidential files only). Implement quarterly reviews of Copilot access grants. Update your data classification policy to explicitly define Copilot eligibility by data tier.

Evidence: If vulnerability is confirmed: preserve the official MSRC advisory and Microsoft's recommended mitigations. Document your containment actions (which licenses disabled, which policies created) and the date implemented. If dismissed: document Microsoft's explanation and your decision to restore Copilot functionality (if applicable). In both cases, conduct a 'lessons learned' review: interview the SOC team and data owners on detection gaps, communication delays, and detection blind spots. Archive this report alongside your incident ticket.

Detection Guidance

NOTE: The following detection guidance is conditional on official confirmation of this vulnerability by Microsoft. Until an official MSRC advisory is published, these queries may not detect the reported attack. Use only for awareness and research purposes. Implement operational detection only after Microsoft confirms the vulnerability and provides technical indicators or analysis.

Hypothetical Approach (pending confirmation): Query Microsoft 365 Unified Audit Logs for Copilot activity events (RecordType: CopilotInteraction) correlated with file-open events in Excel, especially where the triggering file originated from external email or external sharing. Look for Copilot agent invocations that occur without explicit user prompt input; these would appear as system-initiated Copilot interactions at session start. In Microsoft Defender for Cloud Apps or Defender XDR, create alerts for anomalous data access volume from Excel

processes, particularly where SharePoint Online, OneDrive, or Exchange data is accessed immediately after a file-open event. If Purview audit logging is enabled, filter for SensitivityLabelRead or access events on labeled documents initiated by Copilot service principals. No IOCs (IPs, domains, hashes) have been published in available sources as of 2026-03-11; behavioral detection is the primary available approach until Microsoft releases technical indicators or a formal advisory. **Verification step:** Confirm log availability and retention in your specific Microsoft 365 tenant configuration before relying on these queries. Do not implement operational detection until Microsoft publishes official technical analysis.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1566.001** — Spearphishing Attachment
- **T1059** — Command and Scripting Interpreter
- **T1071** — Application Layer Protocol

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
- **CA-7** — Continuous Monitoring
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

CIS-V8

- **6.1**
- **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
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1566.001	Spearphishing Attachment	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1071	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
Forbes	https://www.forbes.com/sites/daveywinder/2026/03/11/critical-0-clic...	T3
This 'fascinating' Microsoft Excel security flaw teams up ... - TechRadar	https://www.techradar.com/pro/security/this-fascinating-microsoft-e...	T3
Critical Microsoft Excel bug weaponizes Copilot Agent • The Register	https://www.theregister.com/2026/03/10/zeroclick_microsoft_info_dis...	T3
Leveraging Copilot In Excel To Steal Data Without Any User ...	https://pcper.com/2026/03/leveraging-copilot-in-excel-to-steal-data...	T3
Critical 0-Click Microsoft Excel Security Bug Lets Copilot Steal Data	https://www.linkedin.com/posts/dlross_critical-0-click-microsoft-ex...	T3
EchoLeak: The Zero-Click Microsoft Copilot Exploit That Changed AI ...	https://www.covertswarm.com/post/echoleak-copilot-exploit	T3

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 2026-03-29 18:35 UTC by TJS Security Command Center