INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:05 UTC

Microsoft Teams Events Portal Information Disclosure Vulnerability (CVE-2026-33823)

CVE VULNERABILITY | CRITICAL | CVSS 9.6

SCC Item ID	SCC-CVE-2026-0140
Type	CVE Vulnerability
CVE ID	CVE-2026-33823
Severity	CRITICAL
CVSS Base Score	9.6
Affected Products	Microsoft Teams (Events Portal component)
Published	2026-05-07T07:00:11
Discovery Source	Msrc Patch Tuesday

Executive Summary

A critical vulnerability (CVE-2026-33823, CVSS 9.6) in the Microsoft Teams Events Portal allows unauthenticated network-based access to sensitive organizational data. Disclosed as part of Microsoft's May 2026 Patch Tuesday, the flaw affects the Events Portal component and carries complete information disclosure (high confidentiality impact) with low attack complexity. Organizations using Microsoft Teams for internal or external event coordination should treat this as a priority patching item.

Technical Analysis

CVE-2026-33823 is an information disclosure vulnerability (CWE-200) in the Microsoft Teams Events Portal component, disclosed May 2026 via MSRC. The CVSS base score of 9.6 indicates a network-exploitable attack vector, low attack complexity, and no required privileges or user interaction, consistent with unauthenticated remote access to protected information. MITRE ATT&CK techniques T1530 (Data from Cloud Storage) and T1552 (Unsecured Credentials) are associated, suggesting the exposed data may include stored event content, attendee information, or session artifacts accessible via cloud-hosted Teams infrastructure. No CVSS vector string is published in the available data; specific exploitation mechanics and affected build versions should be confirmed against the MSRC advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823. EPSS scoring is not yet populated, indicating limited exploitation telemetry at time of publication. CISA KEV listing is not confirmed. Patch availability is sourced from the May 2026 MSRC Update Guide (api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May). No public exploit code or active threat actor attribution is recorded in the item data.

Action Checklist

1. Step 1: Containment, Confirm whether your organization uses the Microsoft Teams Events Portal (distinct from standard Teams meetings). If in use, restrict external access to Events Portal URLs at the network perimeter until the May 2026 patch is applied. Check MSRC advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823 for any interim workarounds published by Microsoft.
2. Step 2: Detection, Query Microsoft 365 Unified Audit Logs for anomalous access events against Teams Events Portal resources, focusing on anonymous or unexpected external principal activity. Review Azure AD sign-in logs for unauthenticated or token-based access patterns aligned with T1530 (cloud storage access) and T1552 (credential object access). Flag event IDs associated with Teams service principals accessing event content outside normal business hours or from unfamiliar IP ranges.
3. Step 3: Eradication, Apply the Microsoft May 2026 Patch Tuesday update addressing CVE-2026-33823. Confirm the specific KB article identifier by referencing the MSRC Update Guide (msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823) before deploying to production, as Teams patches may be server-side only. Validate patch application via Microsoft 365 Admin Center or Intune compliance reporting.
4. Step 4: Recovery, After patching, re-audit Teams Events Portal access logs for any unauthorized data access occurring prior to patch application. Rotate credentials, tokens, or API keys associated with Teams Events Portal integrations if T1552 indicators are present. Verify portal access controls return to expected behavior and confirm no residual unauthorized sessions remain active.
5. Step 5: Post-Incident, Assess whether your organization's Teams Events Portal instances are scoped to internal use only or are externally accessible; reduce external exposure as a standing control. Review cloud application access policies in Microsoft Entra ID (formerly Azure AD) to enforce least-privilege access on collaboration portal components. Log this event as a data point for your next GRC cycle to evaluate Microsoft 365 component-level patching cadence and monitoring coverage.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal/privacy counsel if Microsoft 365 Unified Audit Logs or Azure AD sign-in logs show any unauthenticated or anomalous external principal access to Teams Events Portal resources during the vulnerability window, as this constitutes a potential data disclosure event requiring breach notification assessment under GDPR, HIPAA, or applicable state privacy laws depending on the categories of attendee or organizational data exposed.

Recovery Notes	After patch validation, monitor Microsoft 365 Unified Audit Logs daily for a minimum of 30 days for any recurrence of anomalous Teams Events Portal access patterns — specifically anonymous access attempts or service principal activity outside normal business hours — to detect any attacker persistence established prior to patching. Confirm that all OAuth tokens and API keys rotated during Step 4 have not been re-issued to unauthorized applications by re-running the Entra ID service principal enumeration weekly for the first month. If the data scope assessment from Step 5 identifies PII or regulated data in the exposed Events Portal content, retain all forensic artifacts and engage legal counsel before concluding the incident, as regulatory timelines for breach notification (e.g., 72 hours under GDPR Article 33) may already be running from the date of confirmed or suspected unauthorized access.
Forensic Artifacts	Microsoft 365 Unified Audit Log — filter on Workload:'MicrosoftTeams', Operations containing 'EventsPortal', and UserType:'0' (anonymous) or unexpected external UPN patterns; this is the primary artifact for establishing whether unauthenticated access to Events Portal content occurred and what data was accessed during the CVE-2026-33823 exposure window | Azure AD Sign-in Logs — specifically service principal sign-in entries for the Microsoft Teams application ID scoped to Events Portal resource access, with focus on 'clientAppUsed' values indicating non-interactive or token-only flows (consistent with T1552 credential object access) and 'ipAddress' values outside the organization's known egress ranges | Azure AD Audit Logs — OAuth2 permission grant entries and application permission changes for Teams-integrated apps during the 30-day window preceding the May 2026 Patch Tuesday disclosure, which would indicate if an attacker leveraged CVE-2026-33823 to harvest tokens and escalate permissions within the M365 environment | Network perimeter or NSG flow logs — inbound and outbound connection records to resolved Teams Events Portal IP ranges, capturing source IPs, byte counts, and session durations; unusually high outbound byte counts from Events Portal endpoints to external IPs during the vulnerability window are indicative of data exfiltration aligned with T1530 (Data from Cloud Storage) | Teams Events Portal content inventory — a point-in-time record of event registrations, attendee lists, and shared content accessible via the portal during the exposure window, necessary to scope the categories and volume of organizational data potentially disclosed; this artifact drives the breach notification analysis and cannot be reconstructed retroactively if portal content is modified post-patch

Per-Action IR Details

Step 1: Containment — Confirm whether your organization uses the Microsoft Teams Events Portal (distinct from standard Teams meetings). If in use, restrict external access to Events Portal URLs at the network perimeter until the May 2026 patch is applied. Check MSRC advisory at msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823 for any interim workarounds published by Microsoft.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: If no NGFW with URL filtering is available, use Windows Firewall GPO or iptables to block outbound and inbound connections to Teams Events Portal hostnames (typically *.teams.microsoft.com/events and related subdomains — confirm exact hostnames from MSRC advisory). On a 2-person team: run 'Get-NetFirewallRule' in PowerShell to audit existing block rules, then use 'New-NetFirewallRule -DisplayName BlockTeamsEventsPortal -Direction Outbound -RemoteAddress -Action Block' as a stopgap. Use nslookup or dig to resolve current portal hostnames before blocking.

Evidence: Before implementing network blocks, capture current state: export existing perimeter firewall allow/deny rules for *.teams.microsoft.com scoped to Events Portal paths; run 'netstat -ano' on endpoint systems to identify any active sessions to Teams Events Portal IPs; pull Microsoft 365 Unified Audit Log entries for 'TeamsSessionStarted' and 'EventsPortalAccessed' operation types for the 30 days prior to patch availability (May 2026 Patch Tuesday); preserve a timestamped screenshot or export of Microsoft 365 Admin Center showing current Teams Events Portal enablement status per tenant.

Step 2: Detection — Query Microsoft 365 Unified Audit Logs for anomalous access events against Teams Events Portal resources, focusing on anonymous or unexpected external principal activity. Review Azure AD sign-in logs for unauthenticated or token-based access patterns aligned with T1530 (cloud storage access) and T1552 (credential object access). Flag event IDs associated with Teams service principals accessing event content outside normal business hours or from unfamiliar IP ranges.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use the Microsoft 365 Compliance Center Audit Search (available in all E3/E5 tenants at no additional cost) and filter on Workload:'MicrosoftTeams' with Operations containing 'EventsPortal'. Export results as CSV and parse with PowerShell: 'Import-Csv audit_export.csv | Where-Object { $_.UserType -eq "0" -or $_.UserAgent -match "anonymous" } | Select-Object CreationTime, UserId, ClientIP, Operation | Export-Csv suspicious_events.csv'. For Azure AD sign-in logs without a SIEM, use the Entra ID Sign-in Logs blade filtered on Application:'Microsoft Teams' and Status:'Interrupted' or 'Failure' combined with token-only authentication (no MFA claim). Cross-reference unfamiliar ClientIP values against known office egress ranges using a free IP geolocation API (ip-api.com) via PowerShell Invoke-RestMethod.

Evidence: Preserve the following before and during analysis: (1) Microsoft 365 Unified Audit Log raw export (JSON format preferred) filtered to MicrosoftTeams workload for the full window between CVE disclosure date and patch application — retain at minimum 90 days per NIST AU-11; (2) Azure AD Sign-in Logs for all service principals with 'Teams' in the display name, specifically capturing 'resourceDisplayName', 'ipAddress', 'clientAppUsed', and 'conditionalAccessStatus' fields; (3) any Azure AD audit log entries showing permission grants or OAuth token issuances to Teams Events Portal application IDs in the 30 days preceding disclosure; (4) network flow logs (NSG flow logs in Azure or perimeter firewall logs) showing inbound connections to Teams Events Portal endpoints from IPs outside your known allow-list, correlated with T1530 (Data from Cloud Storage) reconnaissance patterns.

Step 3: Eradication — Apply the Microsoft May 2026 Patch Tuesday update addressing CVE-2026-33823 per the MSRC Update Guide. Confirm the specific KB article or Teams client/service-side update identifier in the MSRC advisory, as Teams cloud components may patch server-side without client action. Validate patch application via Microsoft 365 Admin Center or Intune compliance reporting.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For organizations without Intune or MECM: (1) Verify Teams client version via Teams desktop client > Help > About, and compare against the minimum safe version listed in the MSRC advisory for CVE-2026-33823. (2) Force a Teams client update by closing Teams, navigating to '%localappdata%\Microsoft\Teams\Update.exe' and running 'Update.exe --processStart Teams.exe' from an elevated command prompt — Teams will pull the latest version from Microsoft CDN. (3) For server-side cloud components that patch automatically, confirm remediation by querying the Microsoft Service Health Dashboard (admin.microsoft.com > Health > Service Health) for any posted confirmation of CVE-2026-33823 mitigation deployment. Document the confirmation timestamp as your patch validation record.

Evidence: Before applying the patch, collect: (1) current Teams client version string from all endpoints via PowerShell: 'Get-ItemProperty HKCU:\Software\Microsoft\Office\Teams -Name Version' or parse

'%localappdata%\Microsoft\Teams\current\Teams.exe' file version; (2) a pre-patch snapshot of Microsoft 365 tenant service configuration for the Events Portal feature (exportable via Microsoft Graph API: GET /beta/teamwork/teamsAppSettings); (3) any crash dumps or application event log entries (Windows Event Log, Application channel, Source: Teams) recorded on endpoints during the vulnerability window, which may indicate attempted exploitation triggering unexpected Teams process termination; (4) Intune or MECM compliance report export showing patch compliance state across the endpoint fleet at the moment of eradication — this establishes the remediation baseline for post-incident review.

Step 4: Recovery — After patching, re-audit Teams Events Portal access logs for any unauthorized data access occurring prior to patch application. Rotate credentials, tokens, or API keys associated with Teams Events Portal integrations if T1552 indicators are present. Verify portal access controls return to expected behavior and confirm no residual unauthorized sessions remain active.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without an enterprise PAM or SIEM: (1) Enumerate all service principals and OAuth apps granted delegated or application permissions to Microsoft Teams via PowerShell: 'Get-AzureADServicePrincipal -All $true | Where-Object { $_.DisplayName -match "Teams" } | Select-Object DisplayName, AppId, ObjectId'. (2) For each identified integration, revoke and reissue API keys or rotate client secrets via Entra ID App Registrations > Certificates & Secrets — document the rotation timestamp and new secret expiry. (3) Use Microsoft Graph PowerShell ('Disconnect-MgContext' followed by forced re-authentication) to terminate any active delegated sessions for Teams service principals. (4) Validate portal access behavior post-patch by attempting an unauthenticated browser request to your tenant's Events Portal URL and confirming a 401/403 response is returned rather than data disclosure.

Evidence: Preserve before credential rotation: (1) full export of Azure AD audit logs showing all token issuances, permission grants, and service principal activity against Teams Events Portal application IDs for the entire vulnerability window — this is your chain-of-custody record if regulatory breach notification is required; (2) list of all OAuth tokens currently active for Teams integrations, exported via Microsoft Graph: 'GET /v1.0/oauth2PermissionGrants' filtered to Teams resource; (3) Teams Events Portal event registration data (attendee lists, meeting content, shared files) that was accessible during the exposure window — inventory this data to scope the potential PII/confidential data disclosure for breach impact assessment; (4) network session logs showing any data exfiltration volume (bytes transferred) from Events Portal endpoints to external IPs during the pre-patch window.

Step 5: Post-Incident — Assess whether your organization's Teams Events Portal instances are scoped to internal use only or are externally accessible; reduce external exposure as a standing control. Review cloud application access policies in Microsoft Entra ID (formerly Azure AD) to enforce least-privilege access on collaboration portal components. Log this event as a data point for your next GRC cycle to evaluate Microsoft 365 component-level patching cadence and monitoring coverage.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without a GRC platform: (1) Create a structured lessons-learned record in a shared document capturing: CVE-2026-33823 disclosure date, internal detection date, containment date, and patch date — calculate mean time to detect (MTTD) and mean time to remediate (MTTR) as baseline metrics for M365 component patches. (2) Use Microsoft Secure Score (security.microsoft.com) to identify remaining high-impact recommendations for Teams and Entra ID conditional access that can be implemented at no additional cost. (3) Configure a monthly Microsoft 365 Message Center digest (admin.microsoft.com > Health > Message Center) filtered to 'Security' category to ensure

future MSRC advisories for Teams components are systematically reviewed. (4) Document in your risk register that Teams Events Portal was confirmed as externally accessible (or not) and record the access restriction implemented as a compensating control until such time as architectural review is completed.

Evidence: For the post-incident record, compile and retain: (1) complete timeline artifact package — Unified Audit Log exports, Azure AD sign-in log exports, firewall block rule change records, and patch validation screenshots with timestamps, retained per your organization's incident record retention policy (minimum 3 years recommended for potential regulatory inquiries); (2) the data scope assessment documenting what categories of organizational data (event registrations, attendee PII, meeting content, shared files) were accessible via the Events Portal during the exposure window, to support any required breach notification analysis under applicable regulations; (3) a documented architecture decision record (ADR) or policy update confirming the access scope decision for Teams Events Portal (internal-only vs. external) as a formal configuration baseline going forward per NIST CM-6 (Configuration Settings).

Detection Guidance

Primary log source: Microsoft 365 Unified Audit Log (search for Operations targeting TeamsEvents or EventsPortal workloads). Secondary: Azure AD sign-in logs filtered for Teams service principal activity with anonymous or guest identity context. Behavioral indicators aligned with T1530 include unexpected bulk read operations on Teams-hosted event storage objects. Indicators aligned with T1552 include access to event configuration objects that may contain embedded credentials or API tokens. No public IOCs (IPs, domains, hashes) are available for this vulnerability at time of publication; detection is behavior-based, not signature-based. At publication time (May 2026), Microsoft's audit log documentation for the Teams Events Portal component may still be emerging; consult the MSRC advisory and contact Microsoft Support if audit events are not visible in expected locations.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1552** — Unsecured Credentials

OWASP-TOP10-2021

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

NIST-800-53R5

- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

CIS-V8

- **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

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1552	Unsecured Credentials	Credential-Access

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42826	T1
Warning Over Critical CopyFail Linux Kernel Vulnerability Now ...	https://www.secureblink.com/cyber-security-news/warning-over-critic...	T3
CVE-2026-3833 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3833	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33823	T1

Generated 2026-05-07 19:05 UTC by TJS Security Command Center