INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-09 06:28 UTC

Teams Federation Phishing: APT29 and UNC6692 Exploit Default Permissive Settings for MFA Manipulation and Initial Access

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0430
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Teams (all versions with external federation enabled), Microsoft 365, Microsoft Entra Privileged Identity Management, Palo Alto Networks Cortex (telemetry source)
Published	2026-06-08T23:00:45+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

APT29 (Cloaked Ursa) and UNC6692 are actively exploiting Microsoft Teams' default external federation settings to impersonate IT helpdesk staff, trick employees into approving fraudulent multi-factor authentication prompts, and gain initial access to enterprise environments. The root cause is a permissive-by-default configuration present across millions of Microsoft 365 tenants, not a software vulnerability, meaning any organization that has not explicitly restricted external Teams federation is exposed today. Successful intrusions have led to privilege escalation via Microsoft Entra Privileged Identity Management, putting administrative access, sensitive data, and downstream cloud infrastructure at risk.

Technical Analysis

APT29 and UNC6692 are abusing Microsoft Teams external federation (enabled by default in all M365 tenants) to initiate unsolicited chats with internal employees from attacker-controlled external tenants. Actors impersonate IT helpdesk personas and socially engineer targets into approving fraudulent MFA push notifications (T1621, MFA Request Generation) or providing OTP codes, achieving initial access (T1078, Valid Accounts). Post-access activity targets Microsoft Entra Privileged Identity Management for privilege escalation. The attack chain maps to MITRE ATT&CK techniques T1566.004 (Spearphishing via Service), T1534 (Internal Spearphishing), T1621 (MFA Request Generation), T1556/T1556.006 (Modify Authentication Process), T1539 (Steal Web Session Cookie), T1204.001 (Malicious Link), and T1078 (Valid Accounts). Weakness classification:

CWE-940 (Improper Verification of Source of a Communication Channel), CWE-287 (Improper Authentication), CWE-1390 (Weak Authentication). No CVE is assigned, the attack surface is misconfiguration, not a patched software defect. This campaign has been observed targeting enterprise environments since late 2025. No vendor patch resolves this; remediation requires tenant-level configuration hardening.

Action Checklist

1. Step 1: Containment, Immediately audit Microsoft Teams external access settings in the Microsoft Teams Admin Center (Users > External Access). Restrict external federation to an explicit allowlist of trusted domains or disable external federation entirely if business need cannot be established. This closes the primary attack surface without waiting for a vendor patch. Reference: Microsoft Teams Admin Center > External Access policy.
2. Step 2: Detection, Query Entra ID (Azure AD) sign-in logs and Unified Audit Logs for MFA push approvals (event: 'Sign-in activity', authentication method: 'Microsoft Authenticator') originating at unusual hours or from unfamiliar IPs. Search Teams audit logs for external-tenant chat initiation events targeting users in IT, finance, or executive roles. Look for Entra PIM role activation requests (event: 'Add member to role in PIM completed') within 30 minutes of anomalous MFA approvals. IOC behavioral pattern: external Teams user with display name matching internal IT helpdesk followed by MFA push approval and PIM activation. Map to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, (a) Restrict Teams external access to allowlisted domains only (Microsoft Teams Admin Center). (b) Enable number matching and additional context in Microsoft Authenticator to defeat blind MFA approval (Microsoft Entra > Authentication Methods > Microsoft Authenticator > Configure). (c) Enforce Entra PIM approval workflows requiring a second authorized approver for all privileged role activations. (d) Apply Conditional Access policies requiring compliant, Entra-joined devices for PIM role activation. Reference controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access).
4. Step 4: Recovery, Audit all Entra PIM role activations for the past 90 days for anomalous approvals. Rotate credentials and revoke active sessions for any account that approved an MFA push during a Teams conversation with an external user. Re-validate all privileged account assignments (NIST AC-2, Account Management). Confirm external federation restrictions are enforced by testing from an external tenant. Enable continuous access evaluation in Entra ID to shorten token lifetime for high-risk sessions.
5. Step 5: Post-Incident, Conduct tabletop exercise simulating helpdesk impersonation via Teams. Deliver targeted awareness training to IT staff, finance, and executives on verifying unsolicited Teams contacts from external tenants. Review and update the acceptable use policy for Teams external federation (NIST AC-1, Policy and Procedures). Establish a formal process for employees to report suspicious Teams messages (NIST IR controls). Assess whether Entra PIM approval workflows and Conditional Access policies are documented and auditable against NIST AC-5 (Separation of Duties) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO and legal counsel if any Entra PIM role activation within the 90-day audit window cannot be attributed to an authorized change request, if MFA approval events correlate with data exfiltration indicators in Microsoft 365 Defender or Purview DLP logs, or if the affected tenant is subject to HIPAA, FedRAMP, or financial sector regulations requiring breach notification upon confirmed unauthorized privileged access.
Recovery Notes	After containment, monitor Entra ID sign-in logs and PIM audit logs daily for a minimum of 30 days for re-attempt indicators: new MFA push approvals from IPs not present in the organization's baseline, PIM activation requests citing generic justifications (e.g., 'IT support', 'helpdesk ticket'), or Teams external chat initiations from domains not on the newly enforced allowlist. Re-run `Get-CsTenantFederationConfiguration` weekly for the first month to confirm no policy drift, as Microsoft tenant configuration changes can occasionally revert during service updates. If Continuous Access Evaluation was enabled during recovery, validate that token lifetime reduction is active by checking the `continuousAccessEvaluation` claim in a decoded access token for a high-privilege account.
Forensic Artifacts	Microsoft Entra ID Sign-in Logs (Microsoft Entra portal > Monitoring > Sign-in logs): filter on `authenticationMethodsUsed eq 'MobileAppNotification'` and `status.errorCode eq 0` — successful Authenticator push approvals are the primary forensic record of the MFA fatigue or social engineering event; preserve as CSV with full JSON detail including `ipAddress`, `deviceDetail.deviceId`, `conditionalAccessStatus`, and `appliedConditionalAccessPolicies` fields. | Unified Audit Log — Microsoft Teams record type (Microsoft Purview compliance portal > Audit): operations `MessageCreatedHasLink`, `ChatCreated`, and `MeetingParticipantDetail` with `ExternalAccess: true` field — these capture the attacker's external tenant UPN, display name, and timestamp of initial contact with each victim; the `SenderTenantId` field can be used for threat intelligence correlation against known APT29/UNC6692 infrastructure. | Entra Privileged Identity Management Audit History (`Get-MgIdentityGovernancePrivilegedAccessGroupAssignmentScheduleRequest` or Entra portal > Identity Governance > PIM > Azure AD roles > Resource audit): records of `Add member to role in PIM completed` events with `requestedDateTime`, `requestorId`, `roleDefinitionId`, and `justification` — the justification field frequently contains attacker-supplied text from the social engineering script and is high-value evidence. | Microsoft Entra ID Audit Logs — Authentication Method Changes (Entra portal > Monitoring > Audit logs, service `Authentication Methods`): filter on `Add authentication method` and `Delete authentication method` operations during the compromise window — APT29 TTPs include registering an additional Authenticator device on victim accounts to maintain persistence after initial MFA approval; any new device registration not correlated to a known IT enrollment ticket is a critical indicator. | Microsoft Teams Compliance Export or eDiscovery Hold content (Microsoft Purview > eDiscovery): for confirmed victim accounts, a legal hold will preserve the full Teams message content of the impersonation conversation, including any malicious links, credential harvesting instructions, or urgency-framing language used by the threat actor — this is required for full kill chain reconstruction and is time-sensitive as Teams message retention defaults may purge content within 30 days if no hold is in place.

Per-Action IR Details

Step 1: Containment — Immediately audit Microsoft Teams external access settings in the Microsoft Teams Admin Center (Users > External Access). Restrict external federation to an explicit allowlist of trusted domains or disable external federation entirely if business need cannot be established. This closes the primary attack surface without waiting for a vendor patch. Reference: Microsoft Teams Admin Center > External Access policy.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate the attack vector by modifying the permissive-by-default Teams external federation configuration before the threat actor can initiate additional MFA phishing sessions from external Microsoft 365 tenants.

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without a SIEM or MDM: use PowerShell with the MicrosoftTeams module (`Get-CsTenantFederationConfiguration`) to enumerate the current external access state and confirm whether `AllowFederatedUsers` is set to True. If Teams Admin Center access is restricted to global admins, a delegated Teams Service Administrator account can run `Set-CsTenantFederationConfiguration -AllowFederatedUsers $false` to disable external federation immediately. Document the change with a timestamped screenshot and a before/after PowerShell output for the incident record. This requires no third-party tooling and can be executed by a single analyst in under five minutes.

Evidence: Before modifying external access settings, export the current federation configuration via `Get-CsTenantFederationConfiguration | Export-Csv` to preserve the pre-containment state. Capture Microsoft Teams Admin Center audit log entries under the Unified Audit Log (UAL) in the Microsoft Purview compliance portal, filtering on RecordType `MicrosoftTeams` and operations `TeamsAdminAction` or `ExternalAccessSettingsChanged`, covering at least 90 days prior to containment. This establishes whether federation was intentionally configured or left at default, and provides evidence of any prior policy changes that may indicate attacker pre-positioning.

Step 2: Detection — Query Entra ID (Azure AD) sign-in logs and Unified Audit Logs for MFA push approvals (event: 'Sign-in activity', authentication method: 'Microsoft Authenticator') originating at unusual hours or from unfamiliar IPs. Search Teams audit logs for external-tenant chat initiation events targeting users in IT, finance, or executive roles. Look for Entra PIM role activation requests (event: 'Add member to role in PIM completed') within 30 minutes of anomalous MFA approvals. IOC behavioral pattern: external Teams user with display name matching internal IT helpdesk followed by MFA push approval and PIM activation. Map to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate cross-source signals (Teams federation events, Authenticator push approvals, PIM activations) to reconstruct the APT29/UNC6692 kill chain and identify victim accounts before privilege escalation completes.

Controls: AU-6 (Audit Record Review, Analysis, And Reporting), AU-2 (Event Logging), AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Microsoft's free tooling: (1) Query the Unified Audit Log via PowerShell (`Search-UnifiedAuditLog -RecordType MicrosoftTeams -Operations 'MessageCreatedHasLink','ChatCreated' -StartDate -90`) to identify external-tenant chat initiations. (2) Export Entra ID sign-in logs via `Get-MgAuditLogSignIn` (Microsoft Graph PowerShell SDK, free) filtering on `authenticationMethodsUsed eq 'MobileAppNotification'` and cross-reference against the Entra ID Risky Sign-ins blade. (3) Export PIM audit history from `Get-MgIdentityGovernancePrivilegedAccessGroupAssignmentScheduleRequest` and sort by `createdDateTime` to find activations within a 30-minute window of anomalous MFA approvals. Correlate results manually in a spreadsheet if no SIEM is available. A 2-person team can complete this triage in 2–4 hours.

Evidence: Capture before beginning automated queries: (1) Entra ID sign-in logs (Microsoft Entra portal > Monitoring > Sign-in logs), filtered on authentication method `Microsoft Authenticator` and result `Success`, exported as CSV covering 90 days — these will contain the source IP, device ID, and conditional access policy outcome for each MFA approval. (2) Unified Audit Log entries for `Teams` record type, specifically `MessageCreatedHasLink` and `ChatCreated` operations, which capture the external tenant UPN and display name of the initiating party — the field `ExternalAccess: true` distinguishes cross-tenant messages. (3) Entra PIM audit logs for operation `Add member to role in PIM completed`, which record the requesting UPN, target role, and justification text supplied by the attacker-controlled session — preserve these before any credential rotation invalidates correlation.

Step 3: Eradication — (a) Restrict Teams external access to allowlisted domains only (Microsoft Teams Admin Center). (b) Enable number matching and additional context in Microsoft Authenticator to defeat blind MFA approval (Microsoft Entra > Authentication Methods > Microsoft Authenticator > Configure). (c) Enforce Entra

PIM approval workflows requiring a second authorized approver for all privileged role activations. (d) Apply Conditional Access policies requiring compliant, Entra-joined devices for PIM role activation. Reference controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), D3-MFA (Multi-factor Authentication), D3-CH (Credential Hardening).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the conditions that enabled APT29/UNC6692 initial access — permissive federation, blind push MFA, and ungated PIM activation — so the attack chain cannot be replayed against unidentified victim accounts not yet detected.

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For organizations without Entra ID P2 (required for PIM): (1) As a free compensating control, use Entra ID Conditional Access (included in Microsoft 365 Business Premium and above) to create a policy requiring device compliance for any sign-in to the Microsoft Azure portal or Microsoft Admin portals — this blocks PIM-equivalent role activation from unmanaged or attacker-controlled sessions. (2) Enable Microsoft Authenticator number matching via the Authentication Methods blade (no additional license required as of late 2023 — Microsoft enforced this by default; verify your tenant is not in a managed rollout exemption). (3) For PIM approval workflows without P2, implement an equivalent manual control: require a Slack/Teams message from a second named approver logged in the ticketing system before any privileged role is assigned, and audit this weekly using `Get-MgRoleManagementDirectoryRoleAssignment` exported to CSV.

Evidence: Before executing eradication steps, preserve: (1) A full export of current Entra Conditional Access policies (`Get-MgIdentityConditionalAccessPolicy | ConvertTo-Json -Depth 10`) to document the pre-eradication policy state as forensic baseline. (2) Microsoft Authenticator configuration state from Entra > Authentication Methods > Microsoft Authenticator policy — screenshot or API export confirming whether number matching was disabled at time of attack (this establishes that the attacker exploited a known-weak configuration, relevant for regulatory reporting). (3) PIM role settings export (`Get-MgIdentityGovernancePrivilegedAccessGroupSettings`) documenting that privileged role activations did not require approval — this is direct evidence of the misconfiguration exploited by the threat actor.

Step 4: Recovery — Audit all Entra PIM role activations for the past 90 days for anomalous approvals. Rotate credentials and revoke active sessions for any account that approved an MFA push during a Teams conversation with an external user. Re-validate all privileged account assignments (NIST AC-2 — Account Management). Confirm external federation restrictions are enforced by testing from an external tenant. Enable continuous access evaluation in Entra ID to shorten token lifetime for high-risk sessions. Monitor for re-attempts using D3-LAM (Local Account Monitoring) and D3-CRO (Credential Rotation).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore a verified-clean privilege state by invalidating all sessions and credentials touched during the APT29/UNC6692 compromise window, and confirm that re-hardened controls hold before returning affected accounts to normal operation.

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Session revocation without CASB: run `Revoke-MgUserSignInSession -UserId ` via Microsoft Graph PowerShell for each identified victim account — this immediately invalidates all refresh tokens including those issued to attacker-controlled sessions. Follow with a forced password reset via `Update-MgUser -UserId -PasswordProfile @{ForceChangePasswordNextSignIn=$true}`. To verify external federation restriction is live, create a test Microsoft 365 developer tenant (free 90-day trial) and attempt to initiate a Teams chat to a known internal user — a successful block confirms the allowlist policy is enforced. Log both actions with timestamps in your incident ticket.

Evidence: Before credential rotation, preserve: (1) All active refresh token records for victim accounts via Microsoft Graph (`GET /users/{id}/authentication/methods`) — these establish which authentication methods were registered, whether the attacker registered a new Authenticator device during the compromise window, and provide grounds for

FIDO/passkey enrollment audit. (2) Entra ID audit log entries for `Update user` and `Reset user password` operations in the 90-day window — these may reveal whether the threat actor preemptively changed account recovery options. (3) Entra sign-in logs showing token issuance events post-MFA-approval, specifically `tokenIssuanceStarted` and `conditionalAccessStatus` fields — these document the full session lifecycle of each compromised authentication event for regulatory evidence packages.

Step 5: Post-Incident — Conduct tabletop exercise simulating helpdesk impersonation via Teams. Deliver targeted awareness training to IT staff, finance, and executives on verifying unsolicited Teams contacts from external tenants. Review and update the acceptable use policy for Teams external federation (NIST AC-1 — Policy and Procedures). Establish a formal process for employees to report suspicious Teams messages (NIST IR controls). Assess whether Entra PIM approval workflows and Conditional Access policies are documented and auditable against NIST AC-5 (Separation of Duties) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translate lessons from the APT29/UNC6692 campaign into durable policy, detection, and training improvements that close the human-layer gap exploited by helpdesk impersonation over Teams external federation.

Controls: NIST AC-1 (Policy And Procedures), NIST AC-5 (Separation Of Duties), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For organizations without a dedicated security awareness platform: build the tabletop scenario using Microsoft Teams itself — create a test external tenant and have a red team member impersonate IT helpdesk by crafting a display name matching your internal helpdesk alias, then walk IT and finance staff through recognizing the `External` badge on the Teams chat header and the correct escalation path (e.g., call the helpdesk on a known-good number, not via Teams reply). Document all findings in a free Confluence or SharePoint page as the formal lessons-learned record. Publish a one-page quick reference card showing what an external Teams contact looks like versus internal, and pin it to the IT helpdesk Teams channel.

Evidence: For the post-incident review record, assemble: (1) The complete PIM activation audit log export covering the incident window — this is the primary evidence artifact for any regulatory disclosure and demonstrates the blast radius of ungatd role activations. (2) Teams UAL export showing the full conversation thread metadata (not message content, which requires legal hold) between external attacker accounts and victim users — specifically the `ExternalAccess`, `SenderTenantId`, and `RecipientUPN` fields, which establish the attacker's tenant of origin for threat intelligence sharing with CISA or sector ISACs. (3) A before/after comparison of the `Get-CsTenantFederationConfiguration` output documenting the configuration state at time of attack versus post-remediation — this serves as audit evidence for NIST AC-1 policy compliance and any subsequent third-party audit.

Detection Guidance

Primary log sources: Microsoft Teams Unified Audit Log, Entra ID Sign-in Logs, Entra PIM Audit Logs.

Key detection patterns:

1. External Teams federation abuse: Filter Teams audit logs for 'ChatCreated' or 'MessageSent' events where the sender domain does not match internal or allowlisted domains, targeting users in privileged or IT roles. Correlate with display names containing 'helpdesk', 'IT support', 'Microsoft support', or similar.

2. MFA fatigue / fraudulent approval: Query Entra ID sign-in logs for MFA push approvals (AuthenticationMethod = 'PhoneAppNotification', Result = 'Success') where the originating IP is not a known corporate egress or registered device, especially within minutes of an external Teams message.

3. PIM privilege escalation: Alert on Entra PIM events 'Add member to role in PIM completed (permanent)' or 'Add member to role in PIM completed (eligible)' occurring within 30 minutes of an anomalous MFA approval event for the same UPN.

4. Session token theft indicator: Look for Entra sign-in events with a successful authentication followed by access from a geographically inconsistent IP within a short window (impossible travel), suggesting cookie or token theft (T1539).

Behavioral IOC: External Teams tenant initiates chat > impersonates IT helpdesk > user approves MFA push > PIM role activated from non-standard IP or device.

Mapped 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).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`External Microsoft Teams tenants impersonating internal IT helpdesk — no specific domains published`	Attacker-controlled M365 tenants used to initiate external Teams federation chats; display names spoofed to match internal IT support personas. No specific IOC domains confirmed in public Unit 42 reporting as of this writing.	LOW

Framework Mappings

MITRE-ATTACK

- **T1539** — Steal Web Session Cookie
- **T1621** — Multi-Factor Authentication Request Generation
- **T1556.006** — Multi-Factor Authentication
- **T1534** — Internal Spearphishing
- **T1078** — Valid Accounts
- **T1566.004** — Spearphishing Voice
- **T1556** — Modify Authentication Process
- **T1204.001** — Malicious Link

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)

- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

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

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1534	Internal Spearphishing	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1566.004	Spearphishing Voice	Initial-Access
T1556	Modify Authentication Process	Credential-Access

Technique ID	Technique Name	Tactic
T1204.001	Malicious Link	Execution

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/microsoft-teams-phishing/	T3
	https://www.komando.com/tips/cybersecurity/microsoft-warns-that-it-...	T3
	https://unit42.paloaltonetworks.com/fifa-world-cup-attack-surface/	T3
	https://unit42.paloaltonetworks.com/ai-software-security-risks/	T3
Palo Alto Cortex Microsoft Teams Integration Vulnerability Patched	https://www.linkedin.com/posts/cybersecurity-news_cybersecuritynews...	T3

Generated 2026-06-09 06:28 UTC by TJS Security Command Center