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

Microsoft Enterprise Security Token Service (ESTS) Spoofing Vulnerability, CVE-2026-40379

CVE VULNERABILITY | CRITICAL | CVSS 9.3

SCC Item ID	SCC-CVE-2026-0142
Type	CVE Vulnerability
CVE ID	CVE-2026-40379
Severity	CRITICAL
CVSS Base Score	9.3
Affected Products	Microsoft Enterprise Security Token Service (ESTS)
Published	2026-05-07T07:00:11
Discovery Source	Msrc Patch Tuesday

Executive Summary

A critical spoofing vulnerability (CVSS 9.3) in Microsoft's Enterprise Security Token Service affects authentication across Microsoft 365, Azure Active Directory, and connected enterprise services. An attacker exploiting this flaw could forge authentication tokens, impersonate users, and access enterprise resources without valid credentials. Organizations running Microsoft identity infrastructure should treat this as a priority patching event.

Technical Analysis

CVE-2026-40379 is a spoofing vulnerability in Microsoft's Enterprise Security Token Service (ESTS), disclosed in the May 2026 Patch Tuesday cycle. ESTS issues and validates authentication tokens across Microsoft 365, Azure Active Directory, and dependent enterprise services. The vulnerability maps to CWE-287 (Improper Authentication) and CWE-290 (Authentication Bypass by Spoofing), indicating a flaw in how the service validates token authenticity or identity assertions. Mapped MITRE ATT&CK techniques include T1528 (Steal Application Access Token), T1550.001 (Use Alternate Authentication Material: Application Access Tokens), T1134 (Access Token Manipulation), and T1134.001 (Token Impersonation/Theft). CVSS base score is 9.3. EPSS score and KEV listing are not confirmed in current source data, and proof-of-concept availability is unconfirmed. Patch reference: Microsoft May 2026 CVRF release. Source: MSRC Update Guide (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40379). NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2026-40379.

Action Checklist

1. Step 1: Containment. Apply the Microsoft May 2026 Patch Tuesday update for ESTS immediately across all systems running Microsoft 365 and Azure Active Directory identity infrastructure. Consult the MSRC Update Guide (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40379) for the specific KB article number applicable to your environment. Prioritize internet-facing and federated identity endpoints.
2. Step 2: Detection. Review Azure AD sign-in logs and Microsoft 365 Unified Audit Logs for anomalous token issuance events. Look for authentication events with unexpected token lifetimes, missing MFA claims, or sign-ins from unfamiliar IP ranges with valid session tokens. Query for token issuance failures and invalid credentials with successful token responses in Azure AD logs. Alert on T1528 and T1550.001 behavioral patterns in your SIEM.
3. Step 3: Eradication. Apply the MSRC-released patch for CVE-2026-40379 per Microsoft's May 2026 guidance (https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May). Revoke existing OAuth tokens and refresh tokens for high-privilege accounts and service principals as a precaution. Rotate secrets for applications registered in Azure AD that interact with ESTS.
4. Step 4: Recovery. After patching, verify ESTS token validation behavior by confirming authentication flows for Microsoft 365 and Azure AD-integrated applications return expected claims. Monitor Azure AD sign-in logs for 72 hours post-patch for residual anomalies. Confirm conditional access policies are enforcing correctly on new token issuances.
5. Step 5: Post-Incident. Review conditional access policy coverage for all Azure AD-integrated applications. Assess whether token lifetime policies are configured to minimize exposure windows. Evaluate whether Continuous Access Evaluation (CAE) is enabled to revoke tokens in near-real-time. Document any gaps in token-based anomaly detection and update detection rules accordingly.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and potentially breach notification workflow if Azure AD sign-in logs confirm successful authentication events matching forged-token indicators (Event ID 50126 with successful token response, missing MFA claims for MFA-required accounts, or OAuth permission grants by anomalous service principals) during the vulnerability exposure window, as these conditions indicate credential-equivalent access to Microsoft 365 and Azure-connected resources that may trigger regulatory notification obligations under GDPR, HIPAA, or applicable state breach laws.

Recovery Notes	Following patch application and token revocation, verify that all Microsoft 365 and Azure AD-integrated applications are re-authenticating cleanly by confirming token claim sets match expected tenant policy baselines — any application silently falling back to legacy authentication protocols (basic auth or ADFS legacy endpoints) may bypass the patched ESTS path and should be disabled immediately. Maintain enhanced monitoring of Azure AD sign-in logs with specific focus on service principal authentication events and OAuth permission grants for a minimum of 14 days post-patch, not merely 72 hours, given that attackers who obtained forged tokens prior to patching may have used them to establish persistent OAuth grants or backdoor service principals that survive the patch. Verify that Continuous Access Evaluation is enforcing token revocation in near-real-time for all CAE-capable applications before declaring recovery complete.
Forensic Artifacts	Azure AD Sign-In Logs (Entra admin center > Monitoring > Sign-in logs): Filter for Event ID 50126 (invalid credentials combined with a successful token response) and entries where 'authenticationMethodsUsed' is null or empty despite a 'Success' result status — these are the primary indicators of ESTS token forgery exploitation specific to CVE-2026-40379. | Microsoft 365 Unified Audit Log — 'Add OAuth2PermissionGrant' and 'Add service principal credentials' operations: An attacker who successfully forged ESTS tokens would likely use the resulting session to create persistent OAuth grants or register backdoor credentials on service principals, leaving these audit events as secondary post-exploitation artifacts. | Azure AD Audit Logs — Token Lifetime and Conditional Access Policy change events: Filter 'Get-AzureADAuditDirectoryLogs' for 'Update policy' operations on 'TokenLifetimePolicy' objects during the exploitation window, as an attacker with forged admin-level tokens may have modified token lifetime policies to extend their access window. | Azure AD risky sign-ins and Identity Protection risk detections (Entra ID Protection > Risky sign-ins): Look specifically for 'unfamiliarFeatures' and 'anonymizedIPAddress' risk event types correlated with successful sign-ins, which would indicate forged ESTS tokens being used from attacker infrastructure — these detections are generated automatically and persist independently of sign-in log retention limits. | Service Principal credential inventory snapshot (via 'Get-AzureADApplication' and 'Get-AzureADServicePrincipal' PowerShell): Capture all application password credentials and certificate credentials with creation timestamps falling within the exploitation window — an attacker with ESTS-forged tokens impersonating a privileged user would have had the ability to add new credentials to existing app registrations, leaving behind persistent access that survives both patching and token revocation.

Per-Action IR Details

Step 1: Containment — Apply the Microsoft May 2026 Patch Tuesday update for ESTS immediately across all systems running Microsoft 365 and Azure Active Directory identity infrastructure. Consult the MSRC Update Guide (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40379) for the specific KB or package identifier. Prioritize internet-facing and federated identity endpoints.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If patching cannot be completed immediately, use Azure AD Conditional Access to block all sign-in attempts that lack MFA claims or originate from non-compliant devices, effectively narrowing the attack surface for forged ESTS tokens. As a zero-cost interim, run the Azure AD PowerShell command 'Get-AzureADAuditSignInLogs | Where-Object { $_.AuthenticationRequirement -eq "singleFactorAuthentication" }' to identify and block single-factor sessions exploitable via spoofed tokens while the patch window is scheduled.

Evidence: Before applying the patch, snapshot the current ESTS service configuration and token issuance policies: export Azure AD token lifetime policies via 'Get-AzureADPolicy | Where-Object { $_.Type -eq "TokenLifetimePolicy" }', capture Azure AD sign-in log exports from the Microsoft Entra admin center (Monitoring > Sign-in logs, filtered to the 72 hours preceding detection), and preserve any existing Conditional Access policy configurations via 'Get-AzureADMSConditionalAccessPolicy' to establish a baseline pre-patch state for comparison.

Step 2: Detection — Review Azure AD sign-in logs and Microsoft 365 Unified Audit Logs for anomalous token issuance events. Look for authentication events with unexpected token lifetimes, missing MFA claims, or sign-ins from unfamiliar IP ranges with valid session tokens. Query for Event ID 50076 (token issuance failures) and 50126 (invalid credentials with successful token response) in Azure AD logs. Alert on T1528 and T1550.001 behavioral patterns in your SIEM.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident

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 (Purview) Unified Audit Log search to filter for 'UserLoggedIn' and 'Add service principal credentials' operations, then export to CSV and parse with PowerShell: 'Import-Csv auditlog.csv | Where-Object { $_.Operation -eq "UserLoggedIn" -and $_.ResultStatus -ne "Success" } | Group-Object UserKey | Where-Object Count -gt 10'. For MITRE T1550.001 (Pass the Token) detection without EDR, deploy the free Sigma rule 'win_pass_the_token.yml' converted to PowerShell-based log queries against local Windows Security logs on hybrid-joined systems.

Evidence: The CVE-2026-40379 exploit would produce a forensic signature of ESTS generating tokens with structurally valid signatures but anomalous claim sets — capture Azure AD sign-in log entries where 'authenticationMethodsUsed' is empty or null despite a successful authentication result, and where 'tokenIssuancePolicy' deviates from the tenant's defined baseline. Export Microsoft 365 Unified Audit Log entries for 'Add OAuth2PermissionGrant' and 'Consent to application' operations (MITRE T1528 — Steal Application Access Token) occurring within the exploitation window, as attackers with forged ESTS tokens would likely escalate by granting persistent OAuth permissions.

Step 3: Eradication — Apply the MSRC-released patch for CVE-2026-40379 per Microsoft's May 2026 CVRF guidance (https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May). Revoke existing OAuth tokens and refresh tokens for high-privilege accounts and service principals as a precaution. Rotate secrets for applications registered in Azure AD that interact with ESTS.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Containment, Eradication, and Recovery: Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management) — via token and credential revocation, CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without automated secrets management tooling, use Azure AD PowerShell to revoke all refresh tokens for privileged accounts: 'Get-AzureADUser | Where-Object { $_.AssignedRoles -ne $null } | ForEach-Object { Revoke-AzureADUserAllRefreshToken -ObjectId $_.ObjectId }'. For service principal secret rotation, enumerate all app registrations with ESTS-touching permissions via 'Get-AzureADApplication | ForEach-Object { Get-AzureADApplicationPasswordCredential -ObjectId $_.ObjectId }' and manually rotate credentials through the Azure portal for any application with token issuance or exchange permissions.

Evidence: Before revoking tokens and rotating secrets, capture a complete inventory of all active refresh tokens and OAuth grants that may have been issued under the vulnerable ESTS: export 'Get-AzureADAuditDirectoryLogs | Where-Object { $_.ActivityDisplayName -eq "Add service principal" -or $_.ActivityDisplayName -eq "Add OAuth2PermissionGrant" }' for the exploitation window, and document all service principals with 'AppRoleAssignment.ReadWrite.All' or 'Application.ReadWrite.All' permissions, as these would be high-value targets for an attacker who forged ESTS tokens to establish persistence.

Step 4: Recovery — After patching, verify ESTS token validation behavior by confirming authentication flows for Microsoft 365 and Azure AD-integrated applications return expected claims. Monitor Azure AD sign-in logs for 72 hours post-patch for residual anomalies. Confirm conditional access policies are enforcing correctly on new token issuances.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Containment, Eradication, and Recovery: Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without automated post-patch validation tooling, use the Microsoft 365 connectivity test portal (testconnectivity.microsoft.com) to manually verify end-to-end authentication flows and confirm tokens returned contain expected claims (UPN, tenant ID, MFA claim). For Conditional Access enforcement verification, run 'Get-AzureADAuditSignInLogs | Where-Object { $_.ConditionalAccessStatus -eq "notApplied" }' against post-patch sign-in logs — any 'notApplied' result on a policy that should fire indicates residual enforcement gaps that could still be exploited via forged tokens.

Evidence: Capture post-patch Azure AD sign-in log entries for a minimum of 72 hours and compare token claim structures against the pre-patch baseline — specifically verify that 'amr' (authentication method reference) claims are present and accurate and that 'acr' (authentication context class reference) values align with your Conditional Access policy requirements. Preserve these post-patch log exports as clean-state forensic baselines for future incident comparison.

Step 5: Post-Incident — Review conditional access policy coverage for all Azure AD-integrated applications. Assess whether token lifetime policies are configured to minimize exposure windows. Evaluate whether Continuous Access Evaluation (CAE) is enabled to revoke tokens in near-real-time. Document any gaps in token-based anomaly detection and update detection rules accordingly.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without commercial SIEM tooling, convert community Sigma rules targeting Azure AD token anomalies (search the SigmaHQ repository for 'azure_ad_token' rules) to native KQL queries deployable in Microsoft Sentinel's free tier or Azure Monitor Log Analytics. To assess CAE enablement at no cost, run 'Get-AzureADMSConditionalAccessPolicy | Select-Object DisplayName, SessionControls' and verify 'continuousAccessEvaluation' is set to 'strictEnforcement' for policies governing high-privilege roles — absent CAE, a forged ESTS token could remain valid for up to 1 hour even after revocation.

Evidence: Compile a lessons-learned artifact set specific to CVE-2026-40379: export the full 30-day Azure AD sign-in log history (the maximum retention for P1/P2 tenants) before it ages out, document all Conditional Access policy gaps identified during the 72-hour post-patch monitoring window, and record any service principals found to have possessed overly broad token exchange permissions — these findings directly inform updated detection rules targeting MITRE T1528 and T1550.001 against ESTS-issued tokens in your environment.

Detection Guidance

Query Azure AD sign-in logs for authentication events that succeed without expected MFA claims, originate from new or unexpected IP addresses with valid tokens, or show unusual token lifetimes. In Microsoft Sentinel, use the SigninLogs and AADNonInteractiveUserSignInLogs tables. Example KQL: SigninLogs | where ResultType == 0 | where AuthenticationDetails !contains 'MFA' | where ConditionalAccessStatus == 'success' |

summarize count() by UserPrincipalName, IPAddress, AppDisplayName. Also alert on service principal sign-ins (AADServicePrincipalSignInLogs) with unexpected resource targets. Monitor for T1528 and T1550.001 patterns: token reuse across geographically inconsistent IPs, service principal tokens used outside expected application contexts. No confirmed IOCs or proof-of-concept indicators are available in current source data.

Framework Mappings

MITRE-ATTACK

- **T1528** — Steal Application Access Token
- **T1550.001** — Application Access Token
- **T1134.001** — Token Impersonation/Theft
- **T1134** — Access Token Manipulation

OWASP-TOP10-2021

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

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)

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
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1528	Steal Application Access Token	Credential-Access

Technique ID	Technique Name	Tactic
T1550.001	Application Access Token	Defense-Evasion
T1134.001	Token Impersonation/Theft	Defense-Evasion
T1134	Access Token Manipulation	Defense-Evasion

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40379	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May	T1
CVE-2026-4079 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-4079	T1
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2026-42379 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-40379	T1

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