INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 18:51 UTC

Microsoft Entra ID Entitlement Management Spoofing Vulnerability (CVE-2026-35431)

CVE VULNERABILITY | CRITICAL | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0074
Type	CVE Vulnerability
CVE ID	CVE-2026-35431
Severity	CRITICAL
CVSS Base Score	10.0
Affected Products	Microsoft Entra ID (Entitlement Management component)
Published	2026-04-23T07:00:00
Discovery Source	Msrc Patch Tuesday

Executive Summary

Microsoft disclosed a critical spoofing vulnerability (CVE-2026-35431, CVSS 10.0) in Entra ID's Entitlement Management component as part of the April 2026 Patch Tuesday release. The flaw could allow an attacker to impersonate identities or manipulate access decisions within Microsoft's cloud identity governance plane, which controls who has access to what across Azure and connected applications. Organizations relying on Entra ID for access reviews, access packages, or identity governance workflows are at elevated risk of unauthorized privilege escalation or access policy bypass.

Technical Analysis

CVE-2026-35431 is a spoofing vulnerability in Microsoft Entra ID's Entitlement Management component, classified CWE-290 (Authentication Bypass by Spoofing). The CVSS base score is reported as 10.0 (Critical), indicating network exploitability, low attack complexity, no privileges required, and likely no user interaction, the most severe possible combination. CVSS vector details are pending full NVD publication. Entitlement Management governs access package assignments, access reviews, and identity lifecycle workflows in Entra ID (formerly Azure AD). A successful exploit could allow an unauthenticated or low-privileged attacker to impersonate identities or manipulate entitlement decisions, mapping to MITRE ATT&CK T1134 (Access Token Manipulation), T1078 (Valid Accounts), and T1556 (Modify Authentication Process). No confirmed exploitation in the wild as of the April 2026 Patch Tuesday disclosure. EPSS score is 0.0 and the vulnerability is not listed in CISA KEV at this time. Patch is available via the Microsoft Security Response Center (MSRC) April 2026 update. Sources: MSRC Update Guide

(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431), NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-35431).

Action Checklist

1. Step 1: Inventory & Assessment. Identify all tenants using Entra ID Entitlement Management. Audit current access package assignments and access review configurations for unexpected changes. Review audit logs for the 30 days prior to patch deployment.
2. Step 2: Detection. Query Microsoft Entra ID audit logs for anomalous entitlement management activity: unexpected access package assignments, access review overrides, or identity governance workflow modifications originating from unfamiliar service principals or IP addresses. Monitor Microsoft Defender for Cloud Apps for Entra ID identity anomalies. Log sources: Entra ID Audit Logs (category: EntitlementManagement), Entra ID Sign-In Logs, and Microsoft Defender XDR identity alerts. Use KQL: AuditLogs | where Category == "EntitlementManagement" | where TimeGenerated > ago(30d) | summarize by InitiatedBy, OperationName.
3. Step 3: Eradication. Confirm with your Microsoft tenant administrator or Microsoft support that the April 2026 Patch Tuesday security update for Entra ID has been deployed to your tenant. Microsoft manages Entra ID as a cloud service; cloud-side patches are typically applied automatically.
4. Step 4: Recovery & Monitoring. After patch deployment confirmation, re-audit all access package assignments and access reviews created or modified within the 30 days prior to patch deployment. Verify no unauthorized identities were granted access. Confirm entitlement management policies match approved baselines. Monitor Entra ID audit logs for continued anomalies for a minimum of 14 days post-deployment.
5. Step 5: Hardening & Post-Remediation Review (execute after 14-day monitoring window). Review identity governance controls for over-permissive access package configurations. Enforce Conditional Access policies requiring compliant devices and MFA for entitlement management administrative actions. Conduct a formal access review across all active access packages. Evaluate whether Privileged Identity Management (PIM) is enforced for all Entra ID administrative roles.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if the 30-day audit in Step 4 identifies any access package assignments granted to external identities or unauthorized internal accounts, as unauthorized identity governance plane manipulation in Entra ID may constitute a breach of least-privilege access controls affecting cloud-connected applications and could trigger regulatory notification obligations under GDPR, HIPAA, or applicable state breach notification laws depending on the data classifications accessible via the compromised access packages.

Recovery Notes	After patch confirmation from Microsoft, revoke all Entra ID sessions and refresh tokens for any service principals or user accounts identified as anomalous actors in the EntitlementManagement audit logs before restoring full external user access package availability. Conduct a Graph API-driven full export of access package assignments weekly for the first month post-recovery and compare against your approved provisioning baseline to detect any persistence mechanisms that may have been established via the spoofing flaw prior to patch deployment. Maintain enhanced monitoring of Entra ID Audit Logs (category: EntitlementManagement) and Defender XDR identity alerts for a minimum of 14 days, extending to 30 days if any anomalous assignments were confirmed during the eradication phase.
Forensic Artifacts	Entra ID Audit Logs (category: EntitlementManagement) — specifically operations 'Add accessPackageAssignment', 'Approve accessPackageAssignmentRequest', 'Update accessPackageAssignmentPolicy', and 'Delete accessPackageAssignmentRequest' with InitiatedBy fields showing unexpected service principals or spoofed identity claims, which are the direct artifact of CVE-2026-35431 exploitation in the governance plane | Entra ID Sign-In Logs filtered for non-interactive sign-ins by service principals that appear in EntitlementManagement audit records — look for client credential flows (no MFA, no device compliance) from IP addresses outside known corporate egress ranges, consistent with an attacker using a spoofed or stolen service principal identity to drive governance API calls | Microsoft Graph API audit trail for '/identityGovernance/entitlementManagement/' endpoint calls — accessible via Entra ID Audit Logs with service 'Microsoft Graph' and correlatable to EntitlementManagement category events by timestamp and principal, capturing the raw API interaction layer where the spoofing mechanism would have been exercised | Access Review completion records ('GET /identityGovernance/accessReviews/instances') for any reviews completed during the suspected exploitation window — CVE-2026-35431's identity spoofing capability could have manipulated review approver identities or auto-apply outcomes, leaving anomalous 'reviewedBy' principal entries that do not match the designated reviewers in the review definition | Azure Active Directory Unified Audit Log (exported from Microsoft Purview compliance portal, Workload: AzureActiveDirectory) for the same timeframe — this provides a secondary, tamper-evident log source corroborating EntitlementManagement events and is critical for forensic integrity given that a spoofing vulnerability in the identity plane raises the possibility that primary Entra audit records could reflect attacker-controlled identity attribution

Per-Action IR Details

Step 1: Containment — Identify all tenants using Entra ID Entitlement Management. Audit current access package assignments and access review configurations for unexpected changes. Consider temporarily restricting external user access packages if operationally feasible until the patch is confirmed applied.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Export the full list of Entra ID Entitlement Management access packages and assignments using Microsoft Graph API: run 'Invoke-MgGraphRequest -Method GET -Uri https://graph.microsoft.com/v1.0/identityGovernance/entitlementManagement/accessPackages' and pipe output to a CSV for manual review. For external user packages specifically, run 'Get-MgEntitlementManagementAccessPackageAssignment | Where-Object {$_.AssignmentState -eq "Delivered"} | Export-Csv assignments_$(Get-Date -Format yyyyMMdd).csv'. A 2-person team can divide tenant enumeration from package-level review in parallel.

Evidence: Before restricting external packages, capture a point-in-time snapshot of the Entra ID Audit Log (category: EntitlementManagement) covering at minimum 30 days prior using Graph API or Entra admin portal export — specifically preserve records for operations 'Add accessPackageAssignment', 'Update accessPackageAssignmentPolicy', and 'Delete accessPackageAssignmentRequest'. Also capture the current state of all access review configurations via 'GET /identityGovernance/accessReviews/definitions' to establish a pre-containment baseline for later eradication comparison.

Step 2: Detection — Query Microsoft Entra ID audit logs for anomalous entitlement management activity: unexpected access package assignments, access review overrides, or identity governance workflow modifications originating from unfamiliar service principals or IP addresses. Monitor Microsoft Defender for Cloud Apps for Entra ID identity anomalies. Log sources: Entra ID Audit Logs (category: EntitlementManagement), Entra ID Sign-In Logs, and Microsoft Defender XDR identity alerts.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without Defender for Cloud Apps, query Entra ID Audit Logs directly via the Azure portal (Entra ID → Monitoring → Audit Logs) filtered to Service: 'Entitlement Management' and Date Range: last 30 days. Export to CSV and use PowerShell to isolate anomalies: 'Import-Csv auditlog.csv | Where-Object {$_.InitiatedBy -notmatch "expected-upn-domain" -or $_.ResultReason -eq "Policy override"} | Select-Object ActivityDateTime, InitiatedBy, TargetResources, Result'. For sign-in correlation, filter Entra Sign-In Logs for the same service principal object IDs identified in the audit export and flag any logins from IP addresses not in your known corporate egress range. Free Sigma rule sigma/rules/cloud/azure/azure_identity_governance_anomaly can be adapted for local log parsing if logs are exported to a SIEM-lite like Elastic free tier.

Evidence: Collect Entra ID Audit Logs (category: EntitlementManagement) filtering for operations 'Add accessPackageAssignment' and 'Approve accessPackageAssignmentRequest' where the initiating actor is a service principal rather than a named user — CVE-2026-35431 is a spoofing flaw, so the attack signature is a legitimate-looking identity governance action attributed to an unexpected or spoofed principal. Also capture Entra Sign-In Logs for all service principals that appear in the EntitlementManagement audit records, noting UserAgent strings, IP geolocation, and token issuance details (specifically non-interactive sign-ins using client credentials that would not trigger MFA).

Step 3: Eradication — Apply the Microsoft April 2026 Patch Tuesday security update for Entra ID via the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431). Microsoft manages Entra ID as a cloud service; confirm with your Microsoft tenant admin or Microsoft support that the fix has been deployed to your tenant, as cloud-side patches may be applied automatically.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Because Entra ID is a Microsoft-managed SaaS service, patch application is not tenant-controlled — confirm deployment status by opening a support ticket with Microsoft Premier/Unified support referencing CVE-2026-35431 and requesting written confirmation of patch deployment timestamp for your tenant. If Microsoft support is unavailable, monitor the Microsoft 365 Service Health Dashboard (admin.microsoft.com → Health → Service Health) and the MSRC advisory page for deployment confirmation notices. Document the confirmation response with timestamp as your patch verification record for audit evidence. Note: the URL in the advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431) should be validated by a human operator before treating it as authoritative, as this CVE ID is not yet in my verified training data.

Evidence: Before confirming eradication complete, re-export Entra ID Audit Logs for EntitlementManagement operations post-patch and diff against the pre-patch baseline captured in Step 1 — any 'Add accessPackageAssignment' entries created between initial exploitation window and patch confirmation that do not

correspond to approved requests must be treated as attacker-created and queued for removal in recovery. Preserve the pre-patch and post-patch log exports as forensic evidence in immutable storage (Azure Storage with immutability policy or offline archive) per NIST AU-9 (Protection of Audit Information).

Step 4: Recovery — After patch confirmation, re-audit all access package assignments and access reviews created or modified within the 30 days prior to patch deployment. Verify no unauthorized identities were granted access. Confirm entitlement management policies match approved baselines. Monitor Entra ID audit logs for continued anomalies for a minimum of 14 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run 'Get-MgEntitlementManagementAccessPackageAssignment -Filter "schedule/startDateTime ge 2026-02-03"' (substituting 30 days prior to your patch date) and compare against your approved provisioning records or ITSM ticket history. For any assignment with no corresponding approved request, immediately invoke 'Remove-MgEntitlementManagementAccessPackageAssignmentById -AccessPackageAssignmentId ' and revoke the associated Azure AD session tokens via 'Revoke-MgUserSignInSession -UserId '. Set a recurring daily export of EntitlementManagement audit logs to a shared drive reviewed each morning by one team member for the 14-day monitoring window.

Evidence: During recovery validation, capture a complete export of all active access package assignments via Graph API and cross-reference each assigned identity against your HR system or approved onboarding records — CVE-2026-35431's spoofing mechanism may have allowed assignment of access packages to identities that appear legitimate in Entra ID but were never formally provisioned through your governance process. Also review Entra ID Access Review history for any reviews that were 'auto-applied' or completed with anomalous approver identities during the exploitation window, as a spoofing vulnerability in the governance plane could have manipulated review outcomes to auto-approve unauthorized access.

Step 5: Post-Incident — Review identity governance controls for over-permissive access package configurations. Enforce Conditional Access policies requiring compliant devices and MFA for entitlement management administrative actions. Conduct a formal access review across all active access packages. Evaluate whether Privileged Identity Management (PIM) is enforced for all Entra ID administrative roles.

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 AC-2 (Account Management), NIST IA-2 (Identification and Authentication — Organizational Users), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For Conditional Access without an E5 license, use Entra ID P1 (included in M365 Business Premium) to create a named location policy blocking entitlement management administrative operations from non-corporate IPs, and enforce MFA for any user assigned the Identity Governance Administrator role via a CA policy scoped to that directory role. For PIM evaluation without existing deployment, use the free Entra ID access review feature to identify all users with standing Identity Governance Administrator or Global Administrator role assignments and generate a report — then manually convert standing assignments to eligible-only using the PIM blade in the Entra portal (no additional license cost for PIM on P2; verify current licensing tier before proceeding).

Evidence: For the post-incident lessons learned report, preserve: (1) the full timeline of EntitlementManagement audit log events from 30 days pre-incident through 14 days post-patch; (2) a diff of access package assignment counts and policy configurations before and after the incident window; (3) documentation of which Conditional Access policies were or were not enforced against entitlement management admin operations at the time of exploitation — this gap analysis directly informs the CAP policy hardening in this step and demonstrates whether MFA or device compliance requirements would have blocked the spoofing attack vector for CVE-2026-35431.

Detection Guidance

Query Entra ID Audit Logs filtered to the EntitlementManagement category for the following anomalies: (1) access package assignments created or approved outside normal business hours or by unexpected initiators; (2) access review decisions overridden or completed by accounts not designated as reviewers; (3) identity governance workflow modifications not tied to a change management record. In Microsoft Sentinel, use the AuditLogs table filtered on Category == 'EntitlementManagement' and cross-reference InitiatedBy fields against known administrator accounts. Example KQL query: AuditLogs | where Category == "EntitlementManagement" | where TimeGenerated > ago(30d) | summarize by InitiatedBy, OperationName. In Microsoft Defender for Cloud Apps, enable alerts for impossible travel and anomalous admin activity on Entra ID connectors. There are no published IOCs (IP addresses, domains, or hashes) associated with this CVE at this time; detection relies on behavioral and log-based indicators. Because EPSS is 0.0 and no active exploitation is confirmed, prioritize detection as a precautionary measure while patch deployment proceeds.

Framework Mappings

MITRE-ATTACK

- **T1134** — Access Token Manipulation
- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process

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

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
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1134	Access Token Manipulation	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35431	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Apr	T1
CVE-2026-3431 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3431	T1
March 2026 CVE Landscape: 31 High-Impact Vulnerabilities ...	https://www.recordedfuture.com/blog/march-2026-cve-landscape	T3
SenseLive X3050 - CISA	https://www.cisa.gov/news-events/ics-advisories/icsa-26-111-12	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35431	T1

Generated 2026-04-23 18:51 UTC by TJS Security Command Center