EnCyb

Severity: High

Advisory Type: Threat

Entra ID Delegated OAuth Consent Abuse – Data Exposure Risk

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Attackers can abuse OAuth consent in Microsoft Entra ID by tricking users into authorizing malicious or disguised third-party applications. Once permissions such as **Mail.Read** and **offline_access** are granted, the application can silently and persistently access the user's mailbox without requiring their password. Because non-admin users can often grant consent by default, a single approval can expose sensitive organizational data with minimal detection.

- Active Region: Global
- Affected Sector: Cross-sector (Any Entra ID tenant)
- Affected Product: Microsoft Entra ID (OAuth delegated permission model)
- Severity: High
- Published Date: February 25, 2026

TECHNICAL DETAILS

- **Target:** The primary target is **user mailbox data and Microsoft 365 resources** accessible through delegated OAuth permissions within a Microsoft Entra ID tenant. By obtaining high-risk scopes such as **Mail.Read**, a malicious or unauthorized application can access emails and attachments without stealing credentials, enabling stealthy and persistent data access.

- **Root Cause:** The root cause is **overly permissive user consent settings** combined with the misuse of legitimate OAuth delegated permissions. When non-admin users are allowed to approve high-risk scopes without administrative oversight, attackers can exploit the OAuth trust model to gain persistent access to organizational data.

- **Prerequisite for Exploitation:** Exploitation requires that the tenant allows non-admin consent and that a user is socially engineered into approving a third-party app requesting sensitive scopes such as Mail.Read and offline_access. The absence of strict consent governance or monitoring controls further enables the attack.

IMPACT

- Unauthorized, persistent access to user mailboxes without password compromise
- Silent reading and exfiltration of emails and attachments
- Increased attacker dwell time due to legitimate OAuth token usage
- Bypass of traditional credential-based security detections
- Risk of data breach, regulatory violations, and reputational damage

RECOMMENDATIONS

- Disable or restrict non-admin user consent to third-party OAuth applications
- Require administrator approval for high-risk delegated permissions
- Allow consent only for verified publishers with low-risk scopes
- Regularly review and revoke unnecessary OAuth permission grants
- Implement conditional access policies to limit risky app authorizations

REFERENCE

- https://cybersecuritynews.com/oauth-attacks-in-entra-id-can-leverage-chatgpt/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com