مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Flaw in Microsoft Azure Entra ID

Tracking #:432317738

Date:22-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Security researchers uncovered a critical vulnerability in Microsoft Entra ID (CVE-2025-55241) that could have allowed attackers to compromise every tenant worldwide, including Microsoft 365 and Azure resources.

TECHNICAL DETAILS:

Security researchers uncovered a critical vulnerability in Microsoft Entra ID (CVE-2025-55241) that could have allowed attackers to compromise every tenant worldwide, including Microsoft 365 and Azure resources.
The flaw arose from the combination of undocumented Actor tokens (used for backend service impersonation) and a tenant boundary validation failure in the Azure AD Graph API. With a single Actor token, attackers could impersonate any user—including Global Administrators—across tenants, bypassing Conditional Access, leaving no trace in logs, and persisting for 24 hours.

Microsoft has patched the issue, blocking Actor token abuse in Azure AD Graph and mitigating tenant-wide risk. However, organizations should take immediate steps to review tenant configurations, logs, and trust relationships to identify potential exposure.

Vulnerability Details:

- CVE ID: CVE-2025-55241
- CVSS Score: 10.0 (Critical)
- Affected Component: Microsoft Entra ID (Azure AD) with legacy Azure AD Graph API
- Vulnerability Type: Improper Authentication / Token Validation Failure
- Status: Resolved

Key Technical Issues

1. **Actor Tokens (Undocumented Service Tokens)**
   - JWTs issued by Microsoft backend for impersonation.
   - Could impersonate **any user in any tenant**, bypassing Conditional Access.
   - Valid for **24 hours**, unrevokable, and unlogged.
2. **Azure AD Graph Tenant Validation Flaw**
   - Failed to enforce tenant boundaries.
   - By modifying tenant IDs in tokens, attackers could query **cross-tenant data**.

Attack Path

- Obtain Actor token in lab tenant.
- Alter tenant ID → authenticate as arbitrary users (including Global Admins).
- Bypass all tenant security controls.
- Pivot across **B2B trust relationships**.
- Achieve **full takeover of global tenants** with **no detection**.

Potential Impact

- Global tenant compromise (Microsoft 365, Azure workloads).
- Complete administrative takeover of organizations.
- Cross-tenant lateral movement.
- Stealthy, logless attacks with minimal detection possibility.

RECOMMENDATIONS:

1. **Update & Patching:**
   - No customer-side patching is required; Microsoft has remediated the issue.
   - Ensure tenants are running on the latest Entra ID configuration.
2. **Audit & Detection**
   - Review tenant logs (where available) for suspicious activity, particularly unusual B2B/guest account access or anomalies in Microsoft 365/Azure authentication.
   - Since Actor tokens left little to no logging, correlate with unusual privilege escalation or administrative actions.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERNCES:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55241