Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-55241: Critical Cross-Tenant Privilege Escalation in Microsoft Entra ID

Date of Publication

November 21, 2025

Admiralty Code

A1

TA Number

TA2025355

Summary

First Seen: July 14, 2025
Affected Product: Microsoft Azure Entra ID (formerly Azure Active Directory)
Impact: CVE-2025-55241 is a critical vulnerability in Microsoft Entra ID that allowed attackers to escalate privileges and impersonate any user across tenants, including Global Administrators, by exploiting flaws in undocumented "Actor tokens" and the legacy Azure AD Graph API. The vulnerability bypassed multifactor authentication and Conditional Access, and left minimal logs, making detection difficult. Microsoft rapidly issued a global fix after the July 2025 report, with no evidence of active exploitation found. Organizations are advised to ensure patching, retire deprecated APIs, and review logs for suspicious activity during the affected period. This flaw highlighted significant risks in cloud identity trust boundaries and emphasized the need for strict token validation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55241	Azure Entra ID Elevation of Privilege Vulnerability	Azure Entra ID	✗	✗	✓

Vulnerability Details

#1

CVE-2025-55241 is a critical privilege-escalation vulnerability in Microsoft Entra ID, carrying a maximum CVSS score of 10.0 and discovered by researcher Dirk-Jan Mollema in July 2025. It resulted from the combination of undocumented Microsoft-internal “Actor tokens” and a validation flaw in the legacy Azure AD Graph API. These issues allowed attackers in one tenant to craft tokens that were improperly accepted by other tenants, enabling cross-tenant impersonation of users, including Global Administrators.

#2 The attack chain was unusually simple given its severity. An attacker with access to any Entra ID tenant could obtain an Actor token intended for internal Microsoft service operations. When paired with the Graph API's weak tenant-validation logic, this token enabled the creation of forged identities that authenticated as arbitrary users in other organizations. Actor-token authentication also bypassed MFA and Conditional Access, and because related Graph API calls produced limited logs, initial reconnaissance and exploitation were extremely hard to detect.

#3 Successful impersonation of a Global Administrator could expose or alter sensitive directory data, identity configurations, and application permissions, while granting access to connected Microsoft 365 and Azure resources. The combination of ease, stealth, and potential impact led researchers to warn that nearly all Entra ID tenants were theoretically vulnerable.

#4 Microsoft issued a global hotfix within three days of the July 14 report and deployed additional mitigations by early August. The company reported no evidence of in-the-wild exploitation, though Actor-token usage was not comprehensively logged; Microsoft instead relied on broader service telemetry and administrative-activity patterns to identify signs of abuse. Because the fix was automatically applied, the September 4, 2025 advisory required no customer action. Still, organizations are urged to retire the deprecated Azure AD Graph API, adopt Microsoft Graph, and review administrative logs for suspicious activity during the July to August 2025 period.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-55241	Microsoft Azure Entra ID	cpe:2.3:a:microsoft:entra_id:-:*:*:*:*:*:*:*	CWE-287

Recommendations

Verify Automatic Patch Application: Confirm that your Entra ID tenant received Microsoft's automatic fix that was deployed globally by mid-July 2025. While no customer action was required, administrators should validate their tenant's patch status through the Microsoft 365 admin center or Azure portal to ensure protection is in place.

Migrate from Legacy Azure AD Graph API to Microsoft Graph: Immediately audit and eliminate all remaining dependencies on the legacy Azure AD Graph API (graph.windows.net) in favor of Microsoft Graph. The legacy API was the vulnerable component and Microsoft has accelerated its decommissioning. Review all custom applications, scripts, and integrations to identify and update any code still using the deprecated endpoint.

Conduct Forensic Review of Audit Logs: Search your Entra ID audit logs for July-August 2025 using the provided KQL detection query to identify potential abuse indicators, specifically looking for operations where the display name shows Microsoft services (Exchange, SharePoint, Skype) but the user principal name indicates a regular user account.

Review and Harden Privileged Access Controls: Conduct a comprehensive audit of all privileged role assignments, especially Global Administrator accounts, and review service principal permissions and credentials. Examine any new user accounts, credential additions to existing applications, or permission grants created between July to August 2025, as these were common post-exploitation techniques that would have generated audit logs. Implement least-privilege access principles and enable Privileged Identity Management (PIM) for just-in-time administrative access.

Assess Business-to-Business (B2B) Trust Relationships: Review your tenant's guest user configurations and B2B trust relationships, as the vulnerability could be exploited by hopping across organizational boundaries through guest accounts. Evaluate your default guest user permissions, restrict external collaboration where not business-critical, and implement stricter controls on which external users can enumerate your directory.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0005 Defense Evasion	TA0001 Initial Access	TA0040 Impact
TA0007 Discovery	TA0004 Privilege Escalation	TA0006 Credential Access	T1588 Obtain Capabilities
T1078 Valid Accounts	T1098 Account Manipulation	T1588.005 Exploits	T1562 Impair Defenses
T1078.004 Cloud Accounts	T1098.001 Additional Cloud Credentials	T1087 Account Discovery	T1562.008 Disable Cloud Logs
T1068 Exploitation for Privilege Escalation	T1134.001 Token Impersonation/Theft	T1087.004 Cloud Account	T1134 Access Token Manipulation
T1199 Trusted Relationship	T1588.006 Vulnerabilities	T1621 Multi-Factor Authentication Request Generation	

Patch Details

Microsoft fixed the vulnerability on July 17, 2025 by correcting the token validation logic to prevent cross-tenant Actor token acceptance, then blocked Service Principal-issued Actor tokens for Azure AD Graph API on August 6, 2025. **All patches were automatically applied globally with no customer action required.**

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

References

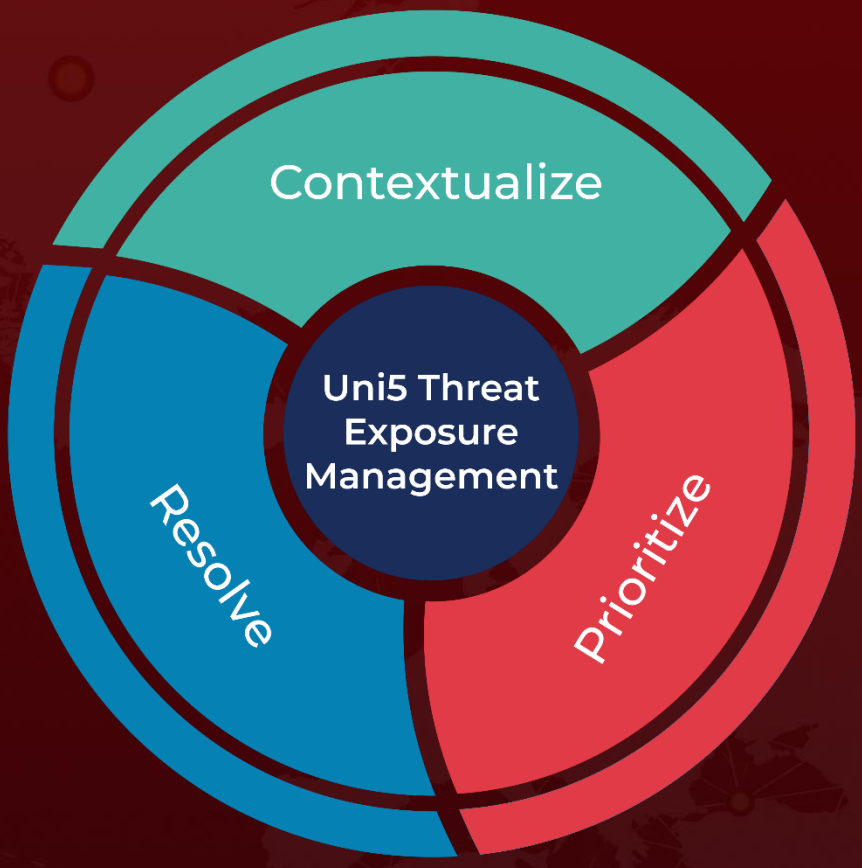
https://dirkjanm.io/obtaining-global-admin-in-every-entra-id-tenant-with-actor-tokens/

https://www.cybermaxx.com/resources/critical-entra-id-vulnerability-cve-2025-55241-microsoft-issues-emergency-fix-for-cross-tenant-token-exploit/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2025 . 8:30 AM

More at www.hivepro.com