CVE-2025-21396: Microsoft Account Elevation of Privilege Vulnerability

Vairav Advisory Report

Date: 2025-01-30

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A vulnerability CVE-2025-21396 has been identified where Missing authorization in Microsoft Account allows an unauthorized attacker to elevate privileges over a network. If exploited this vulnerability can lead to privilege escalation and gaining unauthorized access on machines on the network.

VULNERABILITY DETAILS

CVE-2025-21396

- **Description:** Microsoft identified a flaw in its Microsoft Account infrastructure where adequate authorization checks are missing in the framework. This vulnerability occurs because the application doesn't perform an authorization check when an actor attempts to access a resource.
- **Impact:** This vulnerability allows an unauthorized attacker with network access to hijack the system. The attacker could elevate their privileges to eventually access sensitive features or services designed only for legitimate users with higher permissions.
- **CVSS Score:** 7.5 (High)

AFFECTED VERSIONS

All applications linked to Microsoft accounts are affected by this vulnerability irrespective of version such as:

- Microsoft Azure
- Office 365
- OneDrive
- Xbox

EXPLOIT DETAILS

This vulnerability can be used by an attacker who has access to a Microsoft service that likely uses the Microsoft Account infrastructure to authenticate users. They gain a foothold through a compromised credential or brute force attack. Leveraging the lack of authorization checks, the attacker manipulates the backend service into "thinking" they have higher permissions than they do. With their improperly inflated permissions, the attacker can now perform administrative functions or access sensitive resources without proper oversight.

RECOMMENDED ACTIONS

Microsoft has started rolling out security updates, which they strongly encourage all users and administrators to deploy urgently.

- **For Windows Users:** Go to Settings → Update & Security → Windows Update, and ensure you're running the latest updates.
- **For IT Admins:** Check your endpoints using tools like WSUS or Intune to confirm patch deployment is complete across your network environments.
- **For Developers:** Verify your apps' dependencies and update any libraries or SDKs connected to Microsoft Account services to avoid cascading vulnerabilities.

ADDITIONAL SECURITY MEASURES

- Enable Muti factor authentication to greatly reduce the odds of unauthorized access.
- Use tools like Microsoft Defender for individual users or Sentinel for enterprises to actively scan for unusual activities.
- Update systems and keep an eye out for security advisories.
- Avoid giving accounts more access than necessary.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-21396
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21396
- https://windowsforum.com/threads/cve-2025-21396-critical-microsoft-account-vulnerability-explained.350862/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com