مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Spoofing vulnerability in Microsoft Defender for Identity (MDI)

Tracking #:432317384

Date:16-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a spoofing vulnerability in the Microsoft Defender for Identity (MDI). While not independently exploitable, this flaw can be used in combination with other weaknesses to escalate privileges or exfiltrate credentials.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-26685**
- CVSS score: 6.5 Medium
- A spoofing vulnerability exists in Microsoft Defender for Identity (MDI). This flaw, while not directly exploitable alone, can enable unauthenticated privilege escalation in Active Directory (AD) environments when chained with other known vulnerabilities.
- The vulnerability originates from the SAM-R protocol used by the MDI sensor for lateral movement path discovery, which can be coerced to authenticate to an attacker-controlled system using downgraded NTLM authentication.
- **Impact**
  - Potential for domain privilege escalation via NTLM relay and ADCS exploitation.
  - Risk of impersonation of Domain Service Accounts (DSAs).
  - Unauthorized access to sensitive Active Directory resources.

Affected Products:

- Microsoft Defender for Identity (Classic Sensor)

RECOMMENDATIONS:

- **Migrate to Unified XDR Sensor (v3.x):**
  - Removes reliance on SAM-R queries.
  - Uses **Kerberos-secured WMI** for data collection.
- **Provision DSAs as gMSA accounts**:
  - Reduces risk of successful hash cracking or misuse.
- **Disable LMP Collection** (if not operationally required):
  - Contact Microsoft support for deactivation.
- **Monitor & Detect:**
  - Track **Windows Event ID 4624** for suspicious logon activity.
  - Investigate **DSA authentication events** from unauthorized hosts.

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.

REFERENCES:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26685
- https://www.netspi.com/blog/technical-blog/network-pentesting/microsoft-defender-for-identity-spoofing-cve-2025-26685/