مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Directory Privilege Escalation Vulnerability

Tracking #:432316834

Date:06-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Proof-of-Concept (PoC) exploit has been publicly released for an elevation of privilege vulnerability in Active Directory Domain Services (AD DS) that has been disclosed and patched by Microsoft in its January 2025 security update.

TECHNICAL DETAILS:

A critical elevation of privilege vulnerability (CVE-2025-21293) in Active Directory Domain Services (AD DS) has been disclosed and patched by Microsoft in its January 2025 security update. The vulnerability allows attackers to escalate privileges to SYSTEM level by exploiting the "Network Configuration Operators" group's excessive permissions. A proof-of-concept (PoC) exploit has been publicly released, significantly increasing the risk of exploitation

Vulnerability Overview

- CVE ID: **CVE-2025-21293**
- CVSS 3.1 score of 8.8 (High)
- Public PoC Availability: Yes

The vulnerability resides in the “Network Configuration Operators” group, a default security group in Active Directory. This group is intended to grant limited network configuration privileges without administrative rights. However, due to a misconfiguration, members of this group retain excessive permissions, including the ability to create subkeys under critical service-related registry keys:

- **HKLM\SYSTEM\CurrentControlSet\Services\DnsCache** (DNS Client Service)
- **HKLM\SYSTEM\CurrentControlSet\Services\NetBT** (NetBIOS over TCP/IP Service)

Attackers can exploit this misconfiguration by leveraging Windows Performance Counters, a mechanism used for monitoring system performance. By registering malicious performance counters, attackers can execute arbitrary code with SYSTEM-level privileges, effectively gaining full control over the affected system.

RECOMMENDATIONS:

- Install the January 2025 security update from Microsoft to address CVE-2025-21293 and verify that all domain controllers and Windows Servers are up to date.
- Audit the membership of the “Network Configuration Operators” group and ensure it is empty or contains only authorized users.

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-2025-21293