مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Exploited as Zero Day - Microsoft Exchange Critical Vulnerability

Tracking #:432315617

Date:15-02-2024

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a new critical vulnerability in Microsoft Exchange is being actively exploited by threat actors to gain unauthorized access to affected systems.

## TECHNICAL DETAILS:

Microsoft updated that a newly disclosed critical security flaw in Exchange Server has been actively exploited in the wild.

Microsoft has released a security update to address a critical vulnerability in Exchange Server that is being actively exploited by attackers. Tracked as **CVE-2024-21410** (CVSS Base Score: 9.8 **CRITICAL**), the vulnerability allows remote unauthenticated threat actors to escalate privileges in NTLM relay attacks targeting vulnerable Microsoft Exchange Server versions. Successful exploitation of the flaw could permit an attacker to relay a user's leaked Net-NTLMv2 hash against a susceptible Exchange Server and authenticate as the user.

The vulnerability is mitigated in the Exchange Server 2019 Cumulative Update 14 (CU14), which introduces NTLM credentials Relay Protections. Microsoft has enabled Extended Protection for Authentication (EPA) by default with the Exchange Server 2019 Cumulative Update 14 (CU14) update and PowerShell scripts have been made available to activate Extended Protection on previous versions of Exchange Server.

**Affected Products/Software:**
Microsoft Exchange Server 2019
Microsoft Exchange Server 2016

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Microsoft.

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:

1. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21410