مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in Azure Managed Instance for Apache Cassandra

Tracking #:432316170

Date:21-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that critical security vulnerability (CVE-2024-38175) has been identified in Azure Managed Instance for Apache Cassandra, allowing authenticated attackers to elevate privileges over the network.

TECHNICAL DETAILS:

A critical security vulnerability **(CVE-2024-38175)** has been identified in Azure Managed Instance for Apache Cassandra, allowing authenticated attackers to elevate privileges over the network.

- **CVE ID: CVE-2024-38175**
- **CVSS CVSS v3, Base Score: 9.6, Severity: Critical**
- **Vector:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
- An improper access control vulnerability in the Azure Managed Instance for Apache Cassandra allows an authenticated attacker to elevate privileges over a network.
- An attacker with permissions to deploy User Defined Functions (UDF) in an Azure Managed Instance for Apache Cassandra cluster can send specially crafted requests to the underlying host and extract credentials for managed identities of other clusters on the same host node.
- The compromised credentials enable the attacker to impersonate the victim's managed identity and retrieve information from other clusters hosted on the node which could be outside of the attacker's tenant.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the Apache Cassandra to the fixed version at the earliest.

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-2024-38175