مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerabilities in Docker Desktop

Tracking #:432316278

Date:13-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Docker has released a security update to address multiple remote code execution vulnerabilities in its desktop application.

TECHNICAL DETAILS:

Docker Desktop, a popular application for containerized application development, has been found to contain critical security vulnerabilities that could allow attackers to execute arbitrary code on affected systems.

Vulnerabilities Details:

- **CVE-2024-8695**
  - CVSS Base Score: **9.0 - Critical**
  - A vulnerability in Docker Desktop's handling of extension descriptions and changelogs could allow attackers to execute arbitrary code.

- **CVE-2024-8696**
  - CVSS Base Score: **8.9 - High**
  - A vulnerability in Docker Desktop's handling of publisher-url/additional-urls could allow attackers to execute arbitrary code.

Impact:
Successful exploitation of these vulnerabilities could have allowed an attacker to execute arbitrary code on affected systems. This could lead to unauthorized access, data theft, or other malicious activities.

Affected Versions:
- Docker Desktop before 4.34.2

Fixed Version:
- Docker Desktop 4.34.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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://docs.docker.com/desktop/release-notes/#4342