مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Docker Engine

Tracking #:432316087

Date:25-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Docker released security updates to address a critical vulnerability in Docker Engine.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-41110**| Base Score: 9.9 - Critical | AuthZ bypass and privilege escalation
    - An attacker could exploit a bypass using an API request with Content-Length set to 0, causing the Docker daemon to forward the request without the body to the AuthZ plugin, which might approve the request incorrectly.
    - **Initial fix**: The issue was fixed in Docker Engine v18.09.1 January 2019.
    - **Regression**: The fix was not included in Docker Engine v19.03 or newer versions. This was identified in April 2024 and patches were released for the affected versions on July 23, 2024.

Affected Versions:

- <= v19.03.15, <= v20.10.27, <= v23.0.14, <= v24.0.9, <= v25.0.5, <= v26.0.2, <= v26.1.4, <= v27.0.3, <= v27.1.0

Patched Versions:

- > v23.0.14, > v27.1.0

RECOMMENDATIONS:

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

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://www.docker.com/blog/docker-security-advisory-docker-engine-authz-plugin/