

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## 5-Year-Old Docker Flaw Resurfaces, Allowing Attackers to Slip Past Authorization

Date of Publication

July 25, 2024

Admiralty Code

A1

TA Number

TA2024284




# Summary

**First Seen:** 2018

**Affected Products:** Docker Engine

**Impact:** A critical-severity vulnerability in Docker Engine, identified as CVE-2024-41110, has been found in certain versions. This serious flaw can, in some cases, allow attackers to bypass authorization plugins (AuthZ). Although the issue was first discovered and addressed in Docker Engine v18.09.1, released in January 2019, the fix was not incorporated into later versions, resulting in the reemergence of the vulnerability.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-41110	Docker Engine AuthZ Plugin Bypass Vulnerability	Docker Engine			

# Vulnerability Details

## #1

A critical security flaw has been discovered in Docker Engine, identified as CVE-2024-41110, which may allow attackers to bypass authorization plugins (AuthZ). Initially addressed in Docker Engine v18.09.1 released in January 2019, the fix was not included in subsequent releases, causing the vulnerability to resurface. The bug was rediscovered in April 2024, prompting the release of fixes for all supported Docker Engine versions.

## #2

Docker's default authorization model is all-or-nothing, meaning any user can run any Docker command. To enhance access control, AuthZ plugins can be used, granting or rejecting requests based on authentication and command context. In 2018, a vulnerability was found that allowed attackers to bypass AuthZ plugins using specially crafted API requests, leading to unauthorized operations and privilege escalation. This was fixed in Docker Engine v18.09.1, but the fix did not carry over to later major versions, resulting in a regression affecting users who relied on AuthZ plugins.

## #3

By submitting an API request with the Content-Length set to 0, attackers can exploit the vulnerability CVE-2024-41110. This causes the Docker daemon to route the request without its body, potentially leading to improper acceptance and execution of unauthorized actions. Authorization plugins (AuthZ) typically examine the content of API requests to determine access control. By setting the Content-Length to 0, the request bypasses the AuthZ plugin's inspection, allowing it to be sent to the Docker daemon without its content. This significantly increases the risk of unauthorized activity and privilege escalation.

## #4

Users not relying on AuthZ plugins for authorization, such as those using Mirantis Container Runtime or Docker commercial products, are not impacted by CVE-2024-41110. Affected users should upgrade to Docker Engine v23.0.14 or v27.1.0. Users unable to upgrade to a safe version should disable AuthZ plugins and restrict Docker API access to trusted users.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-41110	Docker Engine: Versions Prior to and v19.03.15, Versions Prior to and v20.10.27, Versions Prior to and v23.0.14, Versions Prior to and v24.0.9, Versions Prior to and v25.0.5, Versions Prior to and v26.0.2, Versions Prior to and v26.1.4, Versions Prior to and v27.0.3, Versions Prior to and v27.1.0	cpe:2.3:a:docker:docker_engine:*:*:*:*:*	CWE-187 CWE-444 CWE-863

## Recommendations



**Update:** Updating Docker Engine to the most current patched version (greater than v23.0.14 or greater than v27.1.0) is advised for users using impacted versions. Additionally, Docker Desktop v4.33 has been released, and users should update to it since it includes a patched version of Docker Engine.



**Deploy Behavioral Analysis Solutions:** Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.



**Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the Docker API to trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0004</u></b> Privilege Escalation	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1068</u></b> Exploitation for Privilege Escalation	

## Patch Details

Users using affected versions are encouraged to update Docker Engine to the most recent patched version (greater than v23.0.14 or greater than v27.1.0). Users should also update to Docker Desktop v4.33, which has been published and contains a fixed version of Docker Engine.

Link: <https://github.com/docker/compose/releases/tag/v2.29.1>

## References

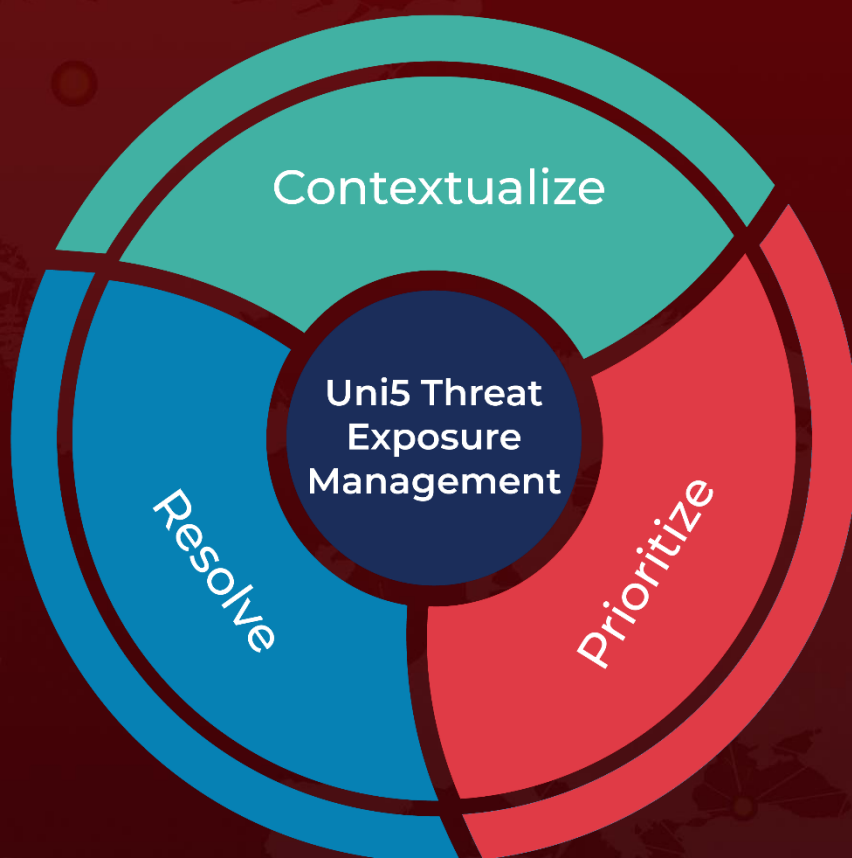
<https://www.docker.com/blog/docker-security-advisory-docker-engine-authz-plugin/>

<https://github.com/moby/moby/security/advisories/GHSA-v23v-6jw2-98fq>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**July 25, 2024 • 7:50 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)