Posted Date: 2025/09/02

[Vulnerability Alert] Docker for Windows has an SSRF vulnerability (CVE-2025-9074)

- Subject: [Vulnerability Alert] Docker for Windows has an SSRF vulnerability (CVE-2025-9074)
- Content:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202508-00000015
  - Docker Desktop for Windows is a container management tool that runs on the Windows system and simplifies application deployment and management through container technology. Docker has released a major security vulnerability update advisory (CVE-2025-9074, CVSS 4.x: 9.3) and a new version. This is a Server-Side Request Forgery (SSRF) vulnerability that allows an attacker to use an API to execute various privileged commands, including controlling other containers and managing images. In addition, the vulnerability also allows mounting the host drive with the same permissions as the user running Docker Desktop.
  - This message is only sent to “county/city network centers”. Please assist in forwarding and notifying the units under your jurisdiction.
- Affected Platforms:
  - Docker Desktop before version 4.44.3 (exclusive).
- Recommended Measures:
  - Update to Docker Desktop version 4.44.3 or later.
- References:
  1. https://docs.docker.com/desktop/release-notes/#4443
  2. https://nvd.nist.gov/vuln/detail/CVE-2025-9074

Computer and Communications Center
Network Systems Group