

Docker Hub patches critical authentication flaw allowing cross-user image manipulation



Docker has patched a critical vulnerability in Docker Hub that allowed attackers to push, pull or delete container images as another user, with no evidence of exploitation found.

- Docker patched a critical authentication flaw in Docker Hub on 30 September 2024
- The vulnerability allowed one user to push, pull or delete container images as another user
- The flaw was located in the feature that converts personal accounts into organisations
- Docker published a security advisory on 12 October 2024 confirming no evidence of exploitation was found
- The vulnerability had existed for approximately two years before remediation

Vulnerability details

Docker has remediated a critical authentication vulnerability in Docker Hub that permitted unauthorised cross-user access to container images. The flaw, patched on 30 September 2024, allowed an attacker to push, pull or delete container images under another user's identity. Docker disclosed the issue in a security advisory published on 12 October 2024.

The vulnerability was present in the account conversion feature that transforms personal Docker Hub accounts into organisational accounts. The flaw had existed for approximately two years before Docker identified and resolved it. According to the vendor's advisory, internal investigation found no evidence that the vulnerability was exploited in the wild during this period.

Implications for regulated institutions

For organisations in the Kingdom using **container registries** as part of their software supply chain, this incident underscores the authentication and access control risks inherent in shared platform services. Container images often embed proprietary code, credentials and configuration data. Unauthorised manipulation of these artefacts could introduce malicious code into production environments or expose sensitive intellectual property.

Regulated institutions relying on Docker Hub or similar public registries should verify that no unauthorised modifications occurred during the vulnerability window. Organisations should also review their container image provenance controls and consider whether private registries or additional image signing mechanisms are warranted for critical workloads.

Remediation status

Docker has confirmed that the patch was applied on 30 September and that all Docker Hub users are now protected. No further action is required from users of the platform itself, though downstream security reviews remain prudent for institutions with compliance obligations under frameworks such as the National Cybersecurity Authority's Essential Cybersecurity Controls or SAMA's Cyber Security Framework.

What to do now

1. Review container image deployment logs from Docker Hub for the period prior to 30 September 2024 to identify any anomalous push, pull or delete activity
2. Verify the integrity and provenance of all container images currently in production that were sourced from Docker Hub during the vulnerability window
3. Assess whether current reliance on public container registries aligns with institutional risk appetite and consider migration to private registries for sensitive workloads
4. Implement or strengthen image signing and verification controls to detect unauthorised modifications to container artefacts

5. Update software supply chain risk assessments to account for authentication vulnerabilities in third-party registry services
6. Brief development and DevOps teams on the incident and reinforce secure container image management practices in line with NCA ECC or SAMA CSF requirements