

Critical Docker Hub Vulnerability Allowed Attacker Impersonation and Image Tampering



Docker disclosed a critical flaw in Docker Hub that permitted attackers to impersonate users and manipulate container images through mishandled personal access tokens during account-to-organization conversions.

- CVE-2026-105445 allowed attackers to reassign personal access tokens without user consent during account-to-organization conversion
- Attackers could pull, push or delete container images in target repositories, creating supply chain risks
- Docker patched the flaw within four hours of confirmation and found no evidence of exploitation across 304,000 analyzed pushes
- Transferred tokens were deactivated on October 8, 2026, and the platform now requires user

consent before ownership changes

- The vulnerability was present from August 26, 2024, until remediation on September 30, 2026

Vulnerability Details

Docker has disclosed CVE-2026-105445, a critical vulnerability in Docker Hub that enabled attackers to impersonate legitimate users and manipulate container images. The flaw stemmed from improper handling of **personal access tokens** during the conversion of individual accounts into organizations.

The attack vector involved creating an account with a personal access token, converting that account into an organization, and designating a target user as the organization owner. Docker Hub would reassign the attacker's token to the target user without changing the secret or obtaining consent. The reassigned token then functioned with the target's permissions at the registry level, allowing attackers to pull, push or delete images in repositories accessible to the victim.

Supply Chain Implications

Docker rated the vulnerability as critical due to its potential impact on software supply chains. Attackers could publish malicious container images under legitimate user names, undermining trust in the container ecosystem. The flaw did not grant web console access or permit changes to account credentials, passwords or two-factor authentication settings, limiting the scope of compromise to registry operations only.

Remediation and Investigation

The vulnerability was introduced on August 26, 2024, and remained present until Docker received a report on September 30, 2026. The company deployed a fix to production within four hours of confirmation. Docker examined 304,000 pushes made with transferred tokens and analyzed high-risk public images, finding no evidence of exploitation. Affected users were notified on October 2, and transferred tokens were deactivated on October 8, except where owners explicitly requested retention. The platform now requires user consent before naming individuals as organization owners and no longer transfers tokens during conversion.

What to do now

1. Audit all Docker Hub accounts and personal access tokens used within your organization to identify any unauthorized conversions or token transfers
2. Review container images pulled or pushed between August 26, 2024, and October 8, 2026, for integrity and authenticity
3. Implement container image verification processes including signature validation before deployment to production environments
4. Establish policies requiring explicit approval workflows for account-to-organization conversions on all

development platforms

5. Update incident response procedures to include supply chain compromise scenarios involving container registries
6. Consider implementing private container registries with enhanced access controls for critical applications under NCA or SAMA frameworks