

apple / container Public

&lt;&gt; Code Issues 204 Pull requests 55 Discussions Actions Projects

# Insecure Hostname Validation Allows HTTP Downgrade Attack

**Moderate** madrob published GHSA-m5rp-xcpf-r8m7 17 hours ago

## Package

 **container** (Swift)

### Affected versions

&lt;=0.12.1

### Patched versions

0.12.3

## Description

### Summary

The `isInternalHost()` function in `RequestScheme.swift` uses insecure string prefix matching to determine whether a registry host should use HTTP or HTTPS. An attacker can craft hostnames (e.g., `localhost.evil.com`) that bypass this check, causing the client to send registry credentials over unencrypted HTTP connections.

### Impact

Users who connect to malicious registries with hostnames matching the bypass patterns will have their registry credentials exposed in plaintext. This affects:

- Registry login operations (username/password)
- Image pull/push operations with authenticated registries
- Any registry interaction using the default `--scheme auto` setting

Bypass patterns include any hostname starting with:

- `localhost` (e.g., `localhost.evil.com`)
- `127.` (e.g., `127.evil.com`)
- `192.168.` (e.g., `192.168.evil.com`)
- `10.` (e.g., `10.evil.com`)
- `172.16.` through `172.31.` (e.g., `172.16.evil.com`)

Severity

Moderate 6.9 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Active

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	None
Availability	None

Subsequent System Impact Metrics

Confidentiality	Low
Integrity	None
Availability	None

[Learn more about base metrics](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:L/SI:N/SA:N

CVE ID

CVE-2026-28909

Weaknesses

No CWEs

Credits

 hackerman70000

Reporter