Edit New issue

Security advisory: Critical vulnerabilities found #127

Open

Labels security

github-actions opened 2 days ago

Security Advisory Report

Open Security advisory: Critical vulnerabilities found #127

Risk Summary

Trivy Results

Target: docker.io/library/alpine:3.10 (alpine 3.10.9)

- **Class:** os-pkgs
- **Type:** alpine

Vulnerability: CVE-2021-36159

- **Package:** apk-tools (2.10.6-r0)
- **Fixed Version:** 2.10.7-r0
- **Severity:** CRITICAL
- **Description:** libfetch before 2021-07-26, as used in apk-tools, xbps, and other products, mishandles numeric strings for the FTP and HTTP protocols. The FTP passive mode implementation allows an out-of-bounds read because strtol is used to parse the relevant numbers into address bytes. It does not check if the line ends prematurely. If it does, the for-loop condition checks for the '\0' terminator one byte too late.
- **References:**
  - https://access.redhat.com/security/cve/CVE-2021-36159
  - https://github.com/freebsd/freebsd-src/commits/main/lib/libfetch
  - https://gitlab.alpinelinux.org/alpine/apk-tools/-/issues/10749
  - https://lists.apache.org/thread.html/r61db8e7dcb56dc000a5387a88f7a473bacec5ee01b9ff3f55308aacc%40%3Cdev.kafka.apache.org%3E

  - https://lists.apache.org/thread.html/r61db8e7dcb56dc000a5387a88f7a473bacec5ee01b9ff3f55308aacc%40%3Cusers.kafka.apache.org%3E
  - https://lists.apache.org/thread.html/rbf4ce74b0d1fa9810dec50ba3ace0caeea677af7c27a97111c06ccb7%40%3Cdev.kafka.apache.org%3E
  - https://lists.apache.org/thread.html/rbf4ce74b0d1fa9810dec50ba3ace0caeea677af7c27a97111c06ccb7%40%3Cusers.kafka.apache.org%3E
  - https://nvd.nist.gov/vuln/detail/CVE-2021-36159
  - https://www.cve.org/CVERecord?id=CVE-2021-36159

Checkov Summary

- **Passed checks:** 38
- **Failed checks:** 52
- **Skipped checks:** 0
- **Parsing errors:** 0

Recommended Actions

- Update vulnerable dependencies.
- Apply available patches or workarounds.

Create sub-issue

github-actions added security 2 days ago

Add a comment

Write Preview

Use Markdown to format your comment

Paste, drop, or click to add files

Close issue Comment

Metadata

Assignees