

VEX Working Group

SBOM-a-Rama

2023-06-14

Art Manion

zmanion@protonmail.com

What is VEX?

Vulnerability Exploitability eXchange (VEX) indicates the status of a software product or component with respect to a vulnerability.

A common VEX use case is to indicate that software is or is not affected by a vulnerability.

- Born from SBOM: How do I convey the status of an upstream component vulnerability in my product?
- Works with SBOM, or independently
- Convey vulnerability status in a more standard way
- One vulnerability, one status, one or more components

Status

Not affected

- No remediation or mitigation is required. The vulnerability does not affect the listed products.

Affected

- Actions are recommended to remediate, mitigate, or otherwise address the vulnerability. The vulnerability affects the listed products.

Fixed

- The listed products contain fixes for the vulnerability.

Under investigation

- The author of the VEX statement or other relevant parties are investigating and have not yet declared a final status.

“Not affected” justifications

Component not present

- The vulnerable subcomponent is not included in the product.

Vulnerable code not present

- The vulnerable subcomponent is included in the product but the vulnerable code is not present.

Vulnerable code not in execute path

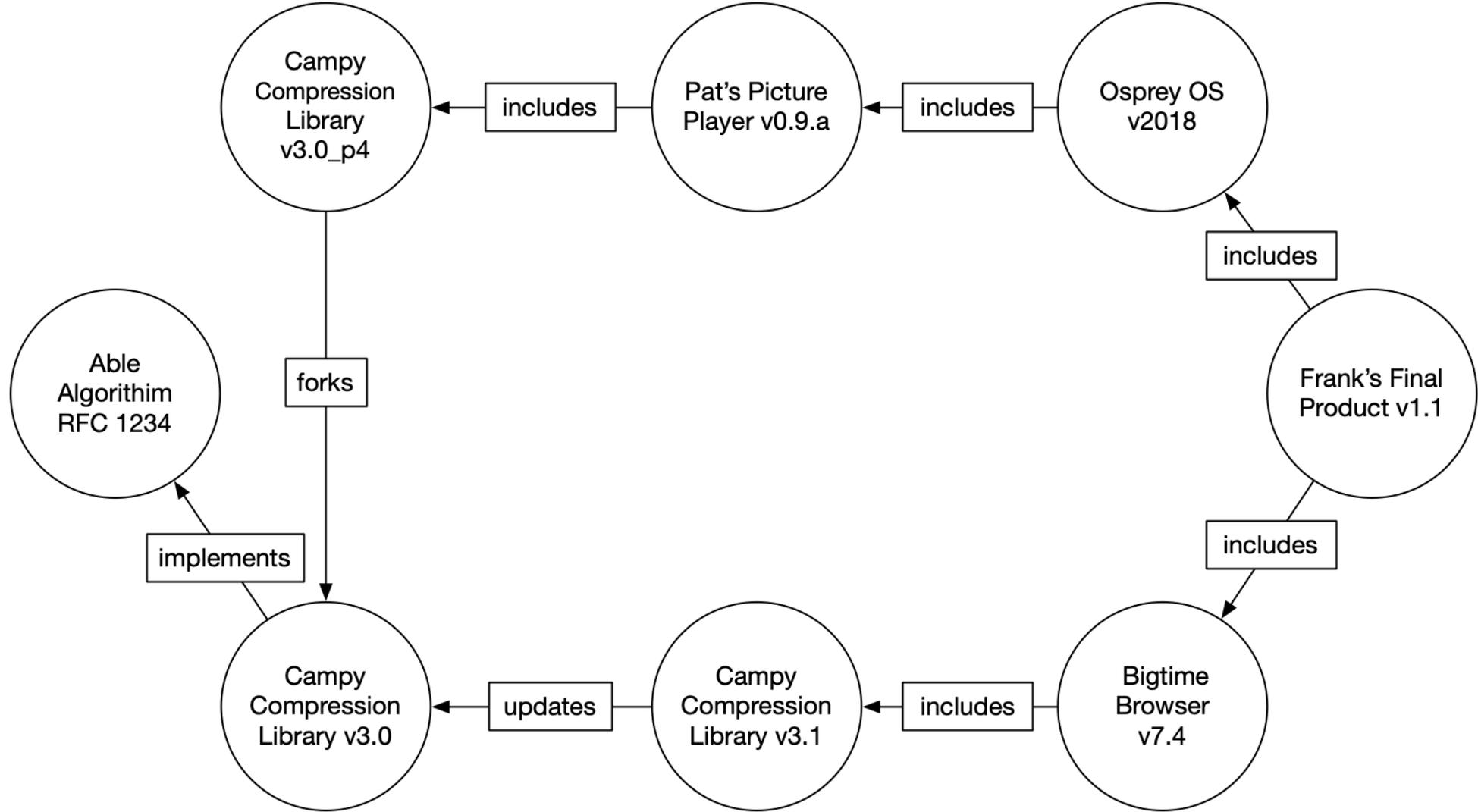
- The vulnerable code (likely in the subcomponent) cannot be executed due to the way it is used by the product.

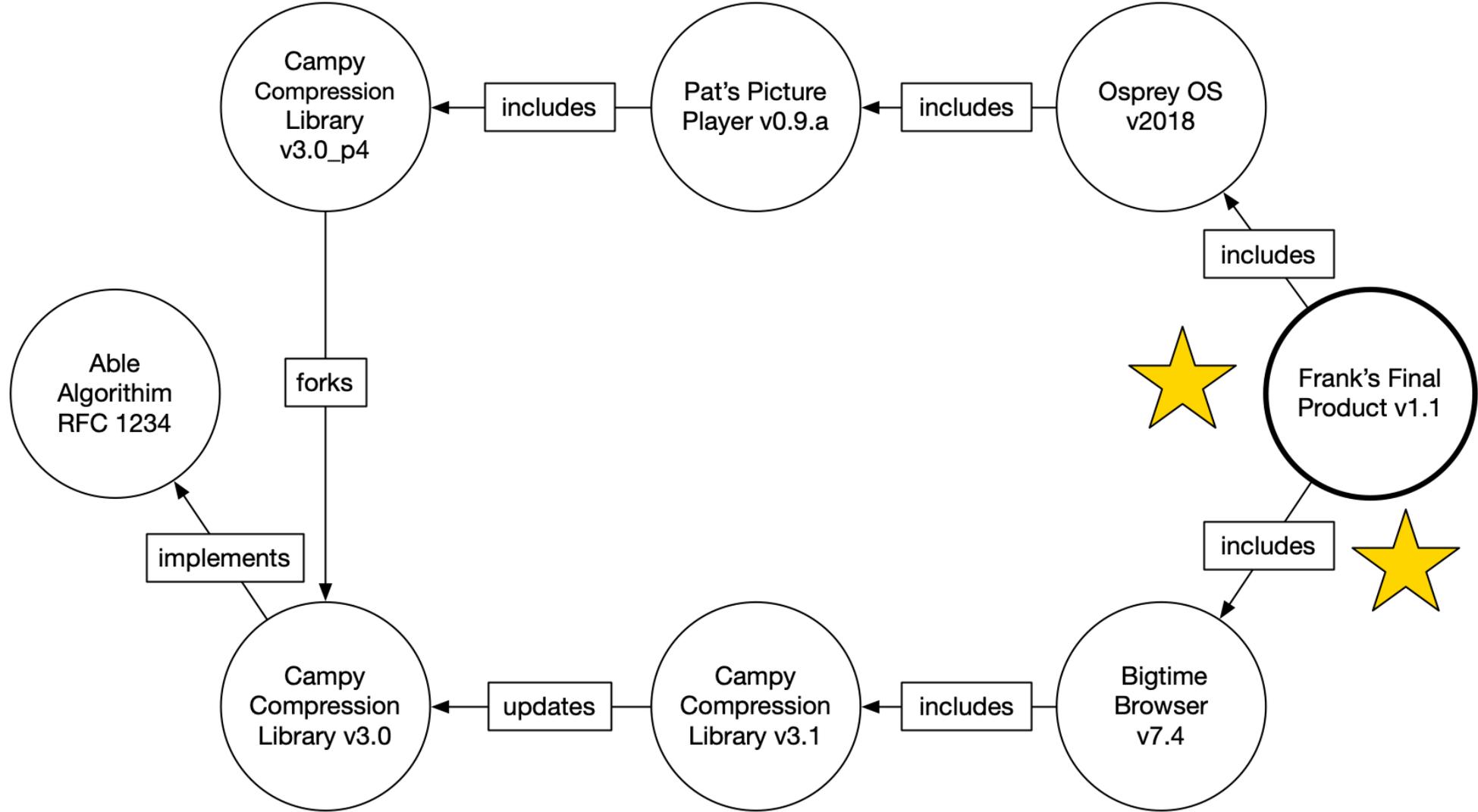
Vulnerable code cannot be controlled by adversary

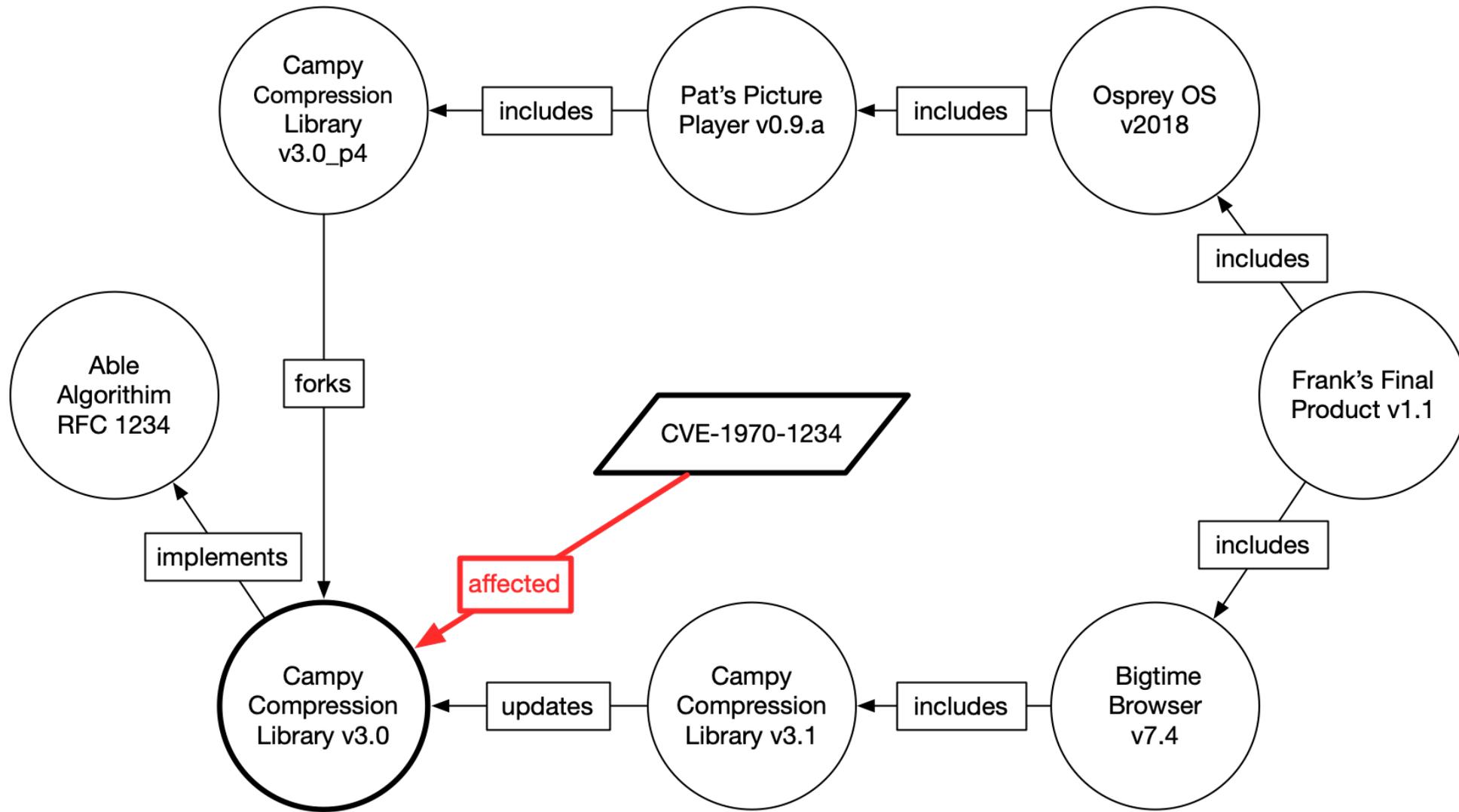
- The vulnerable code is present and used by the product but cannot be controlled by an attacker to exploit the vulnerability.

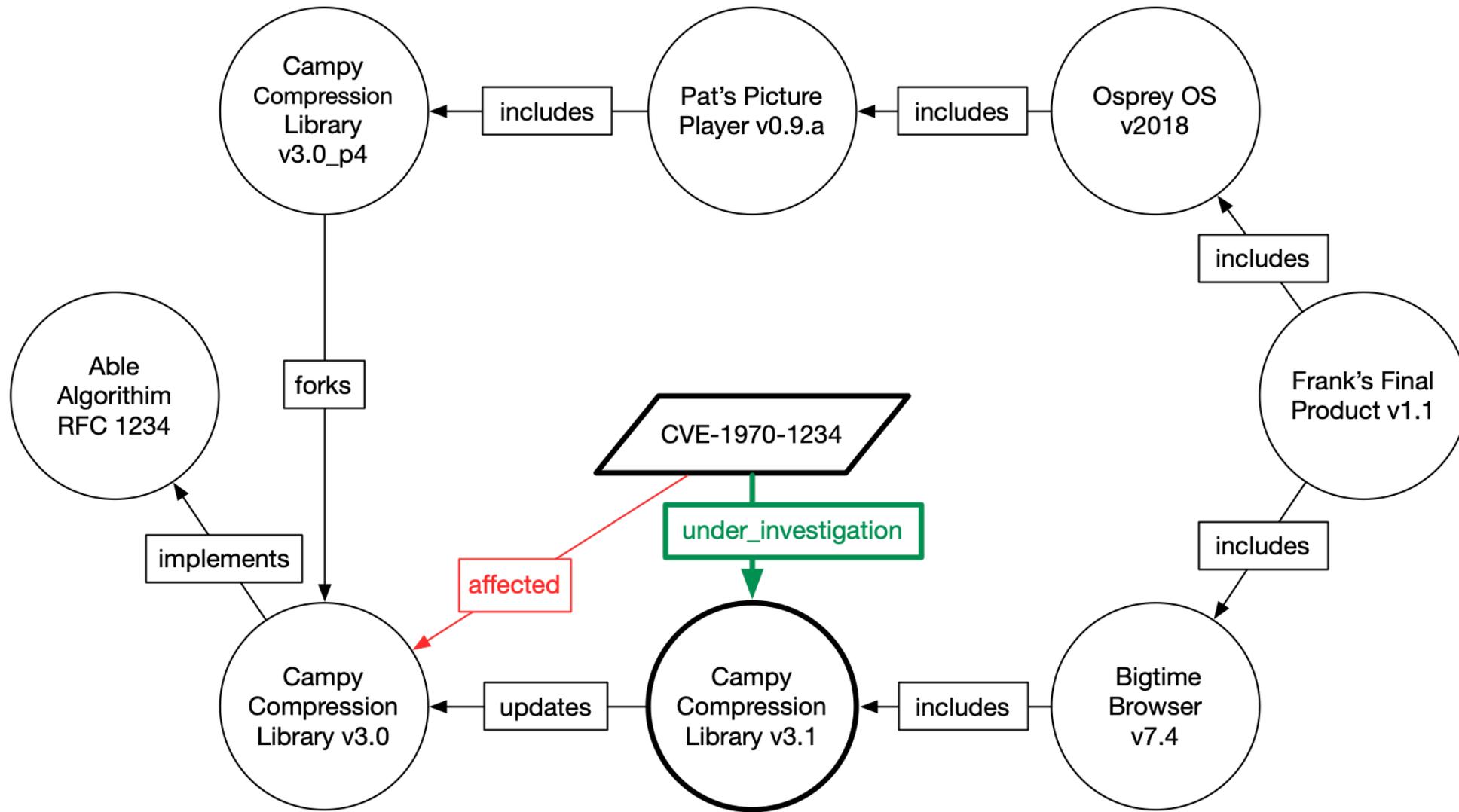
Inline mitigations already exist

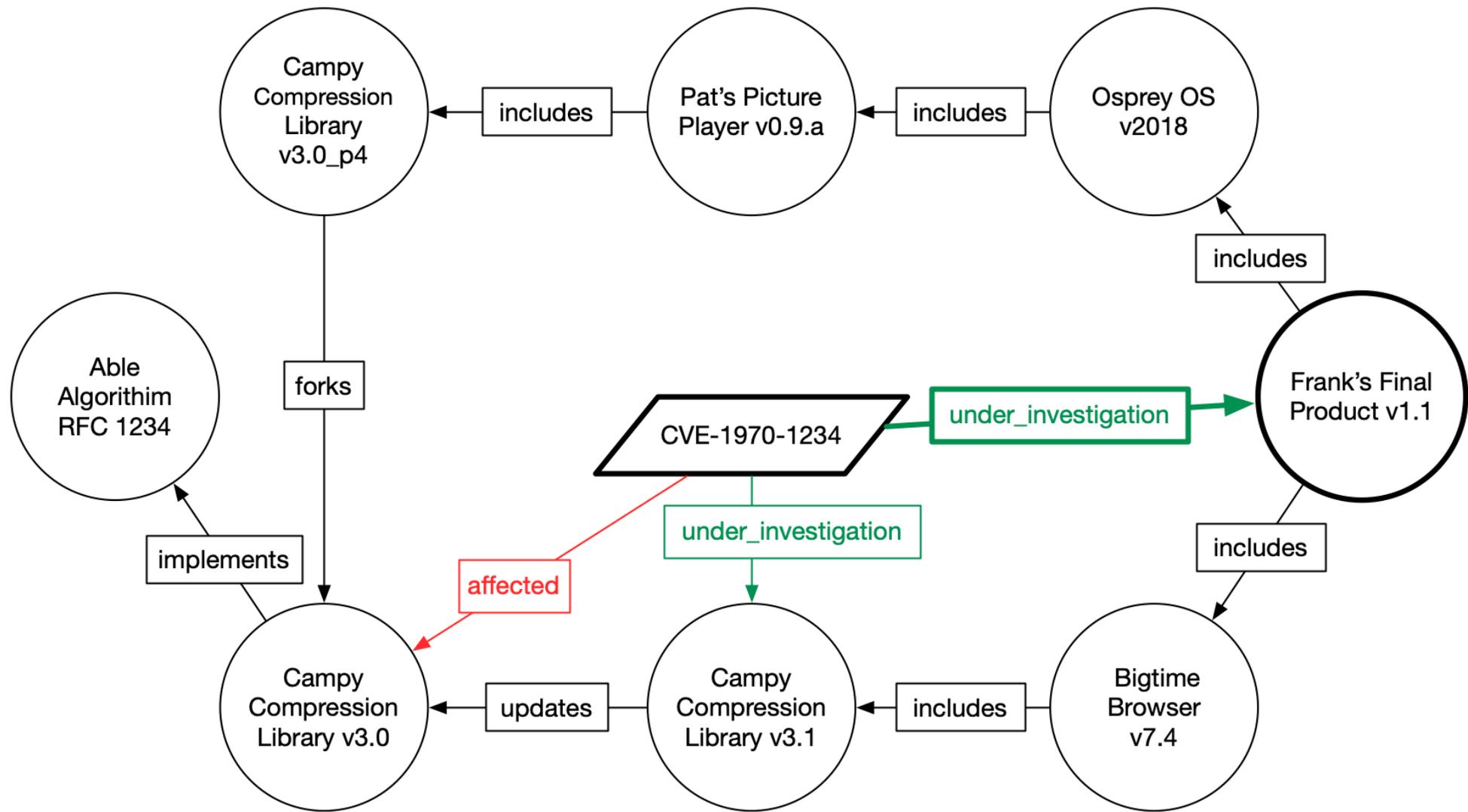
- The product includes built-in protections or features that prevent exploitation of the vulnerability. These built-in protections cannot be subverted by the attacker and cannot be configured or disabled by the user. These mitigations completely prevent exploitation based on known attack vectors.

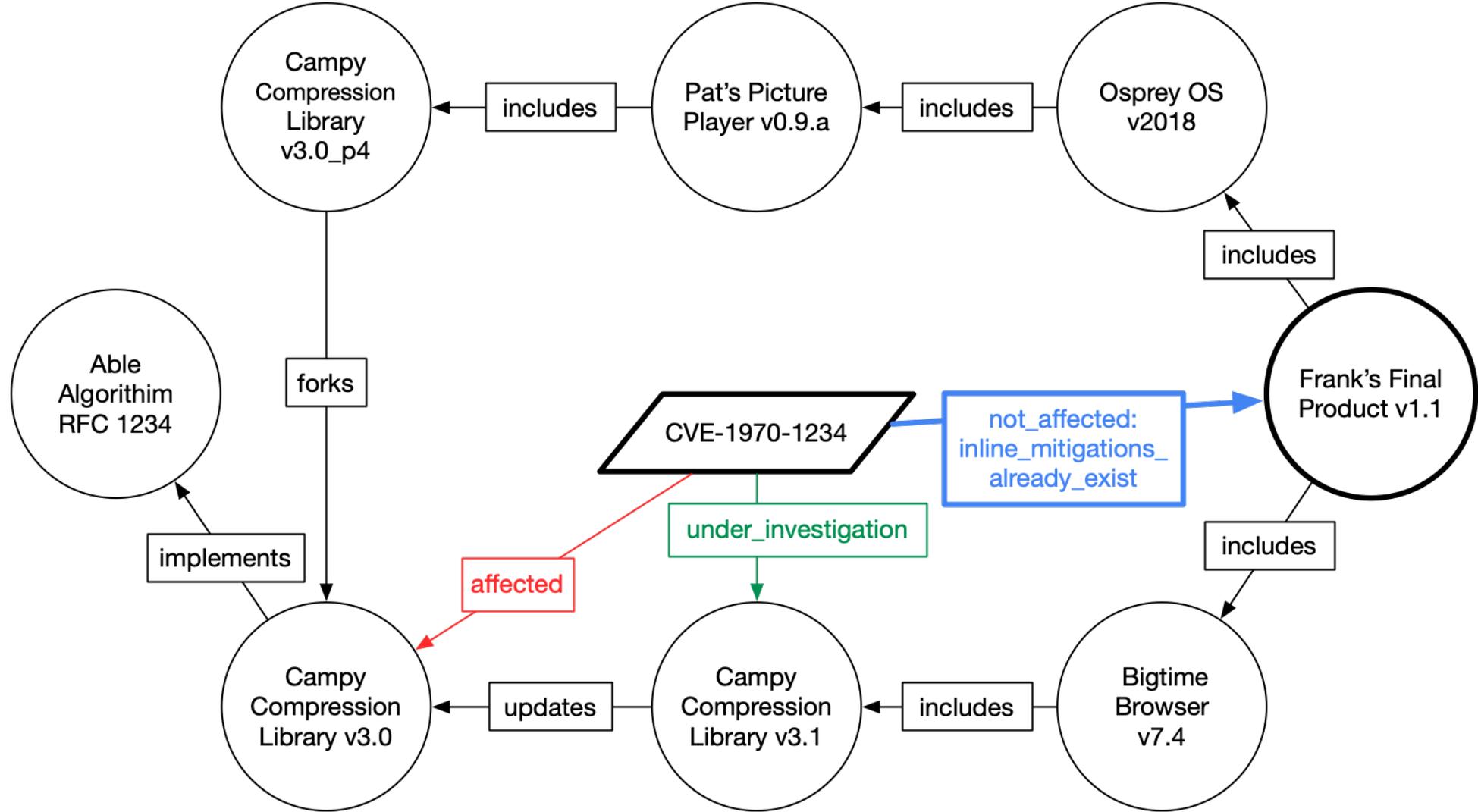


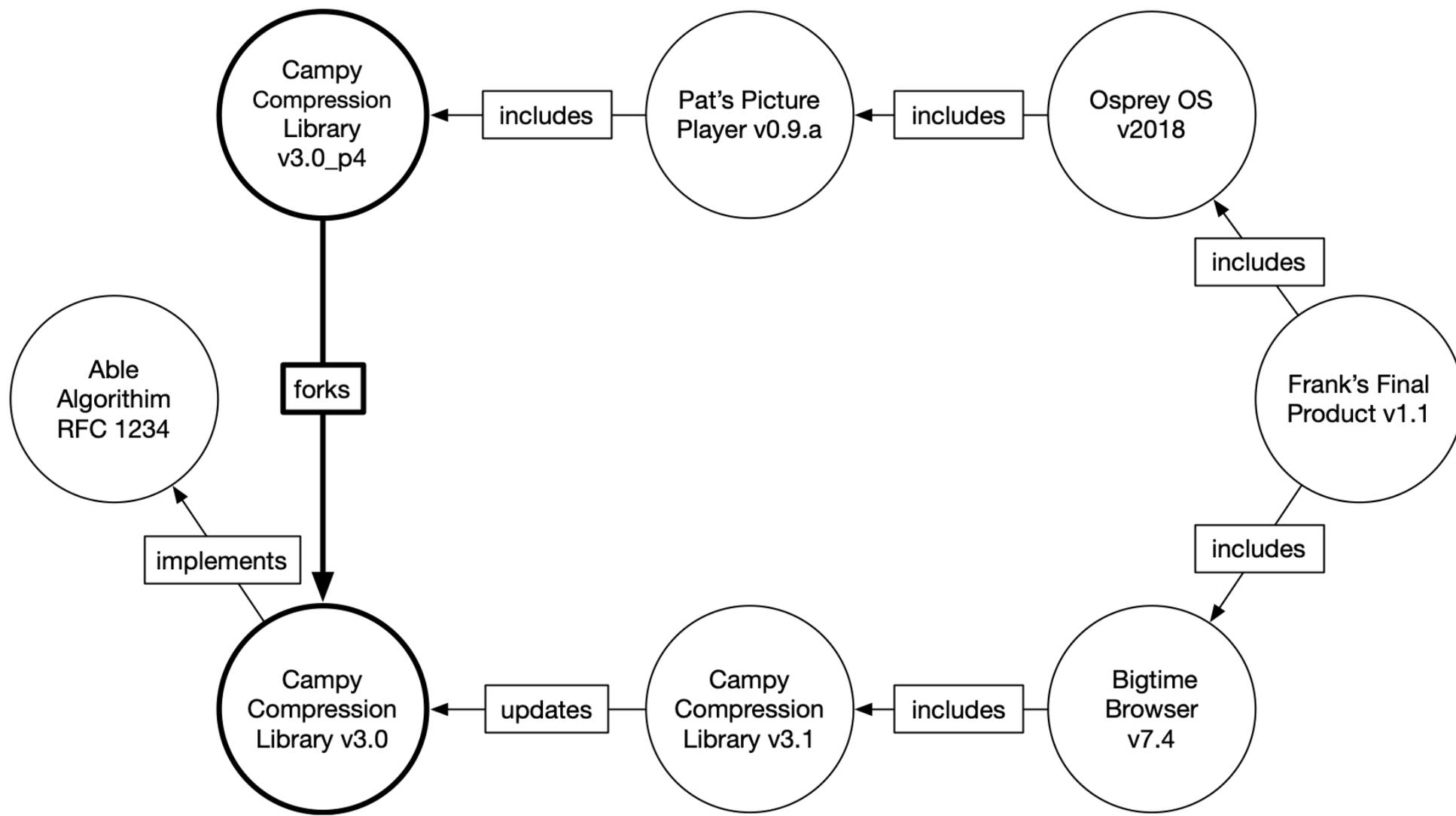


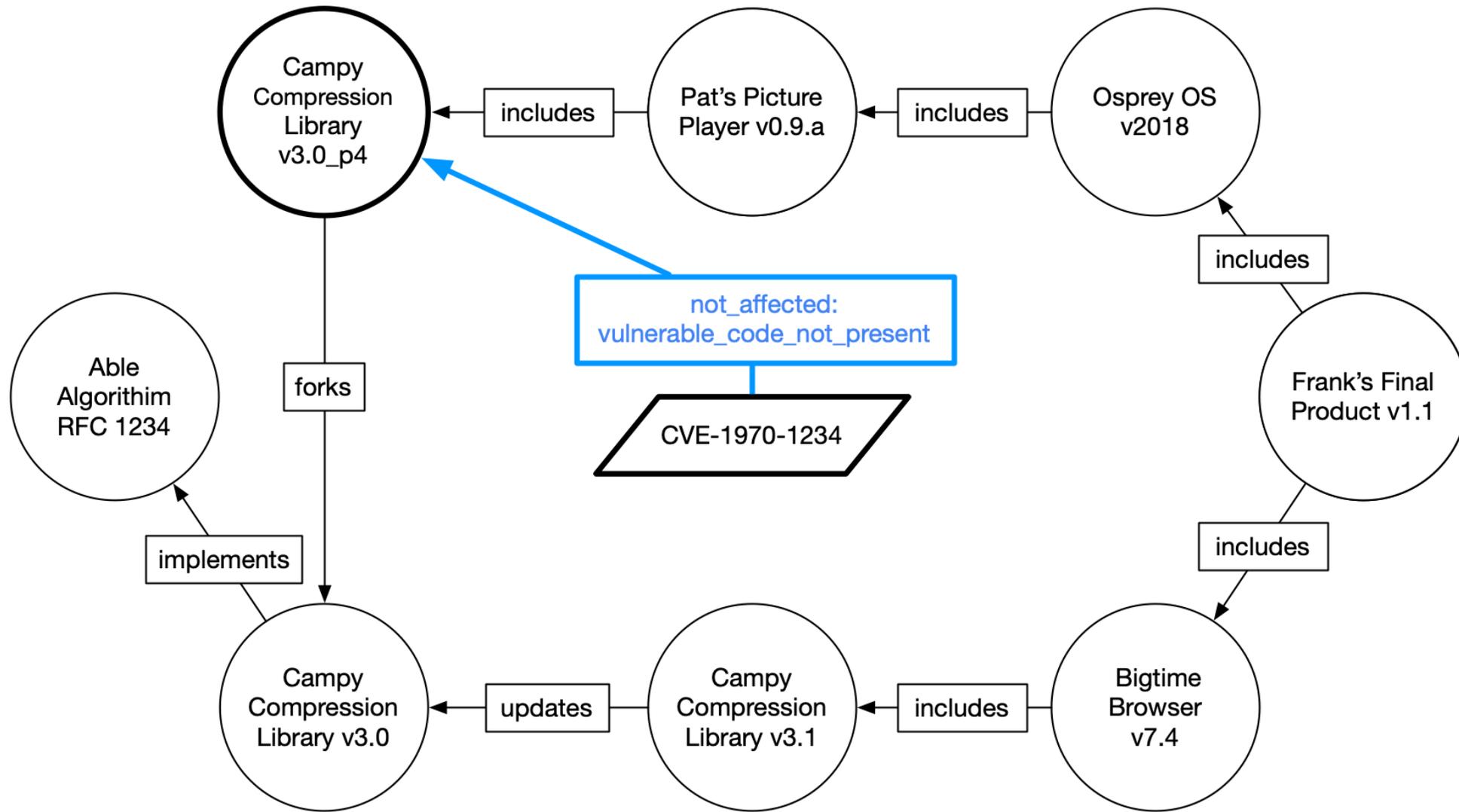


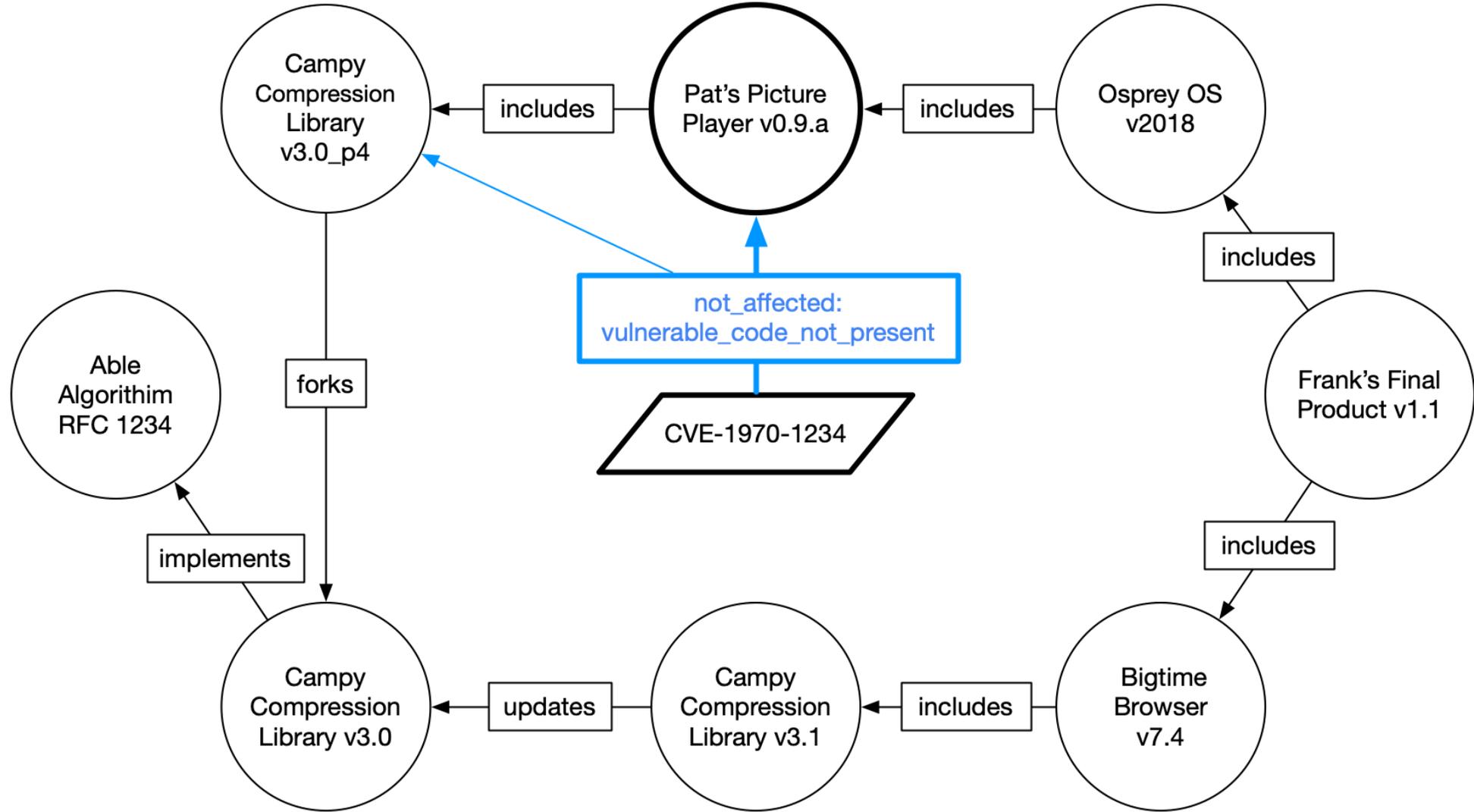


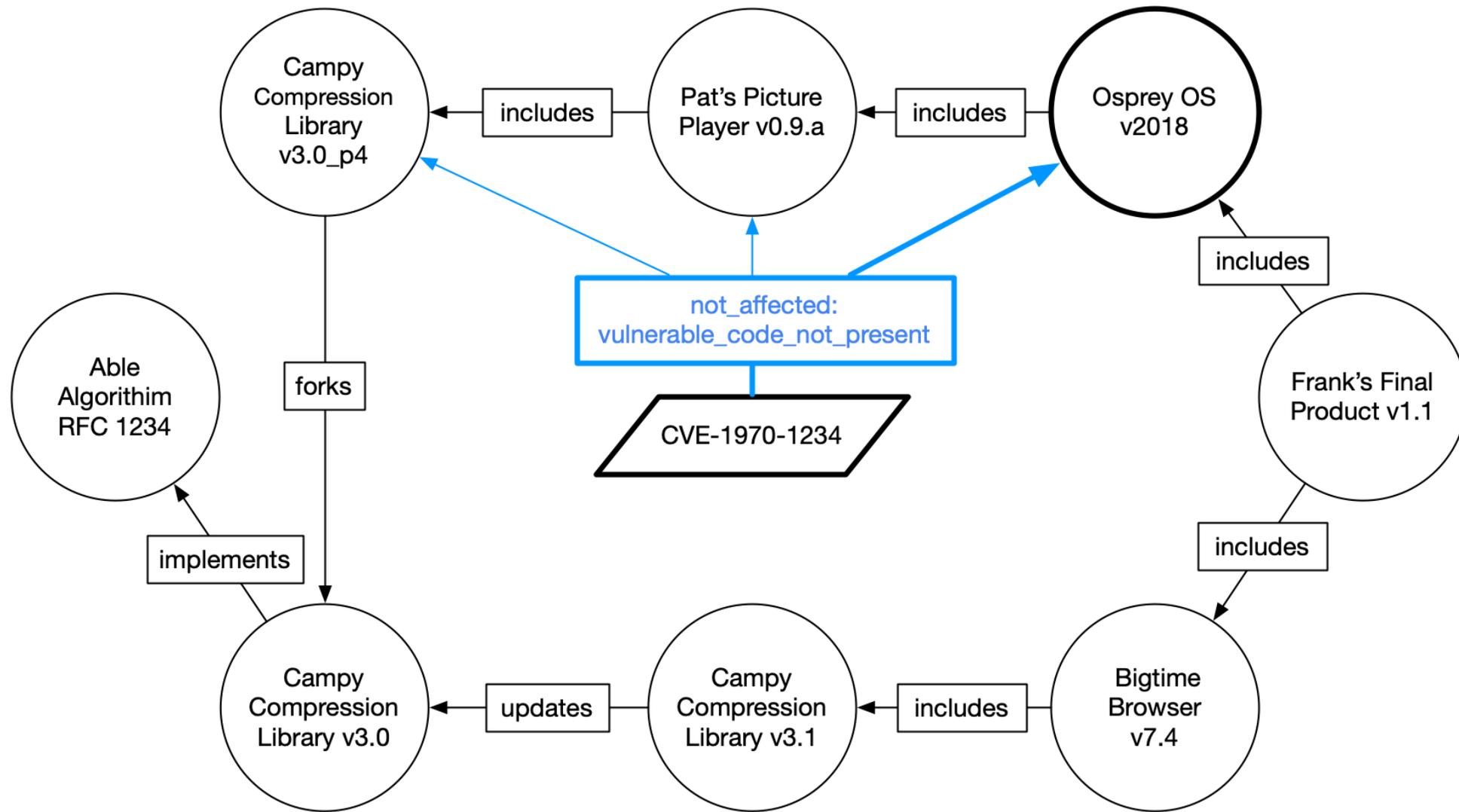


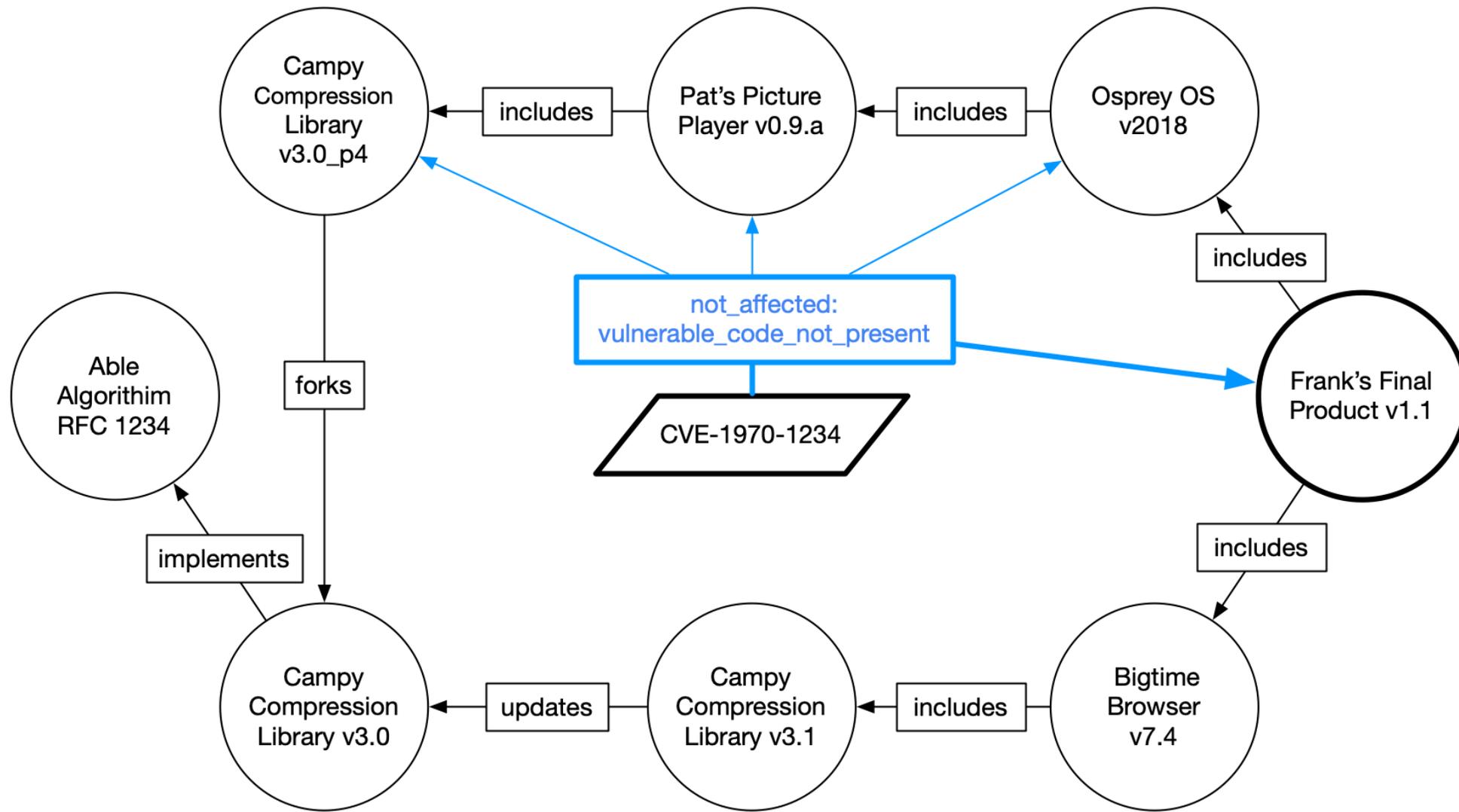


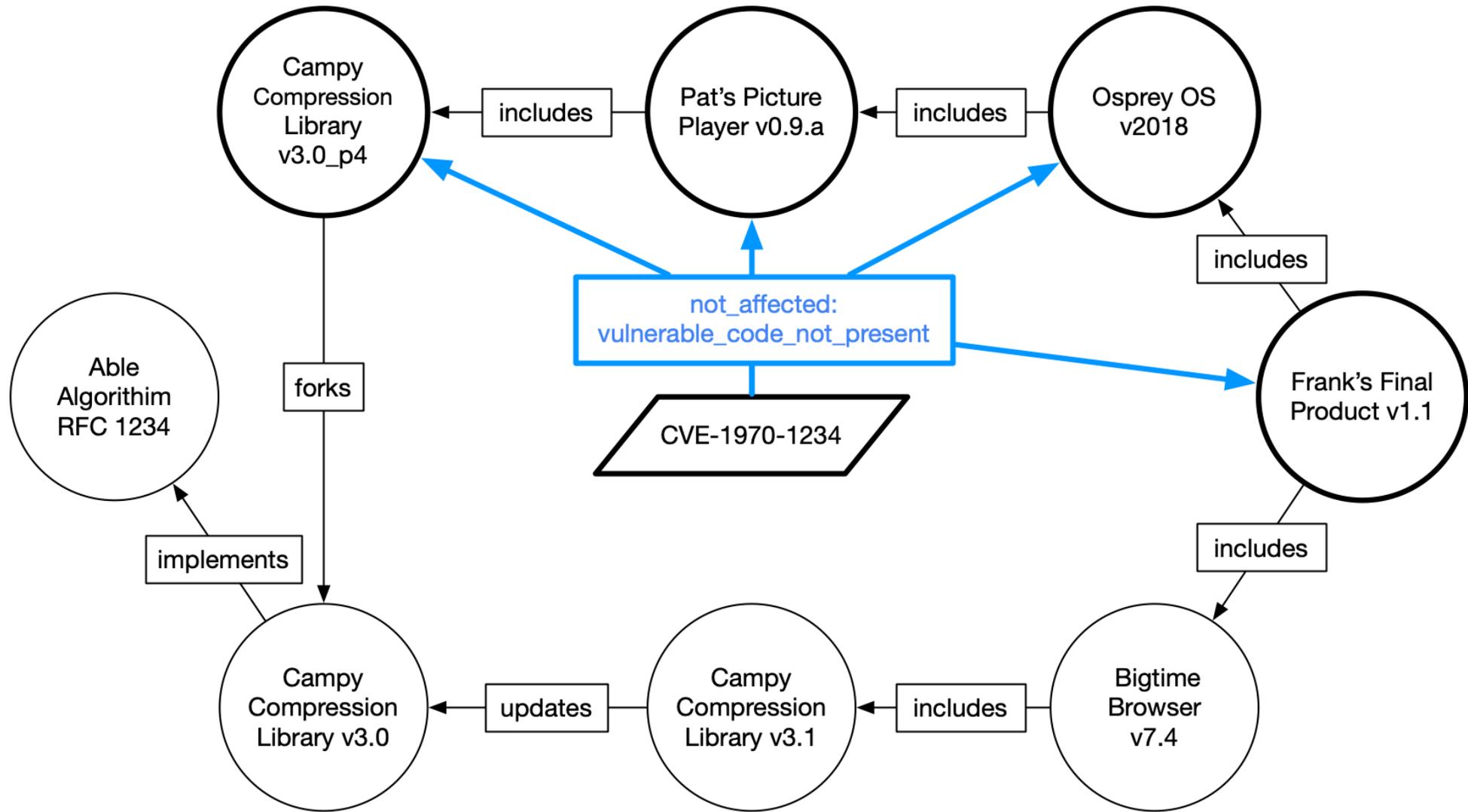


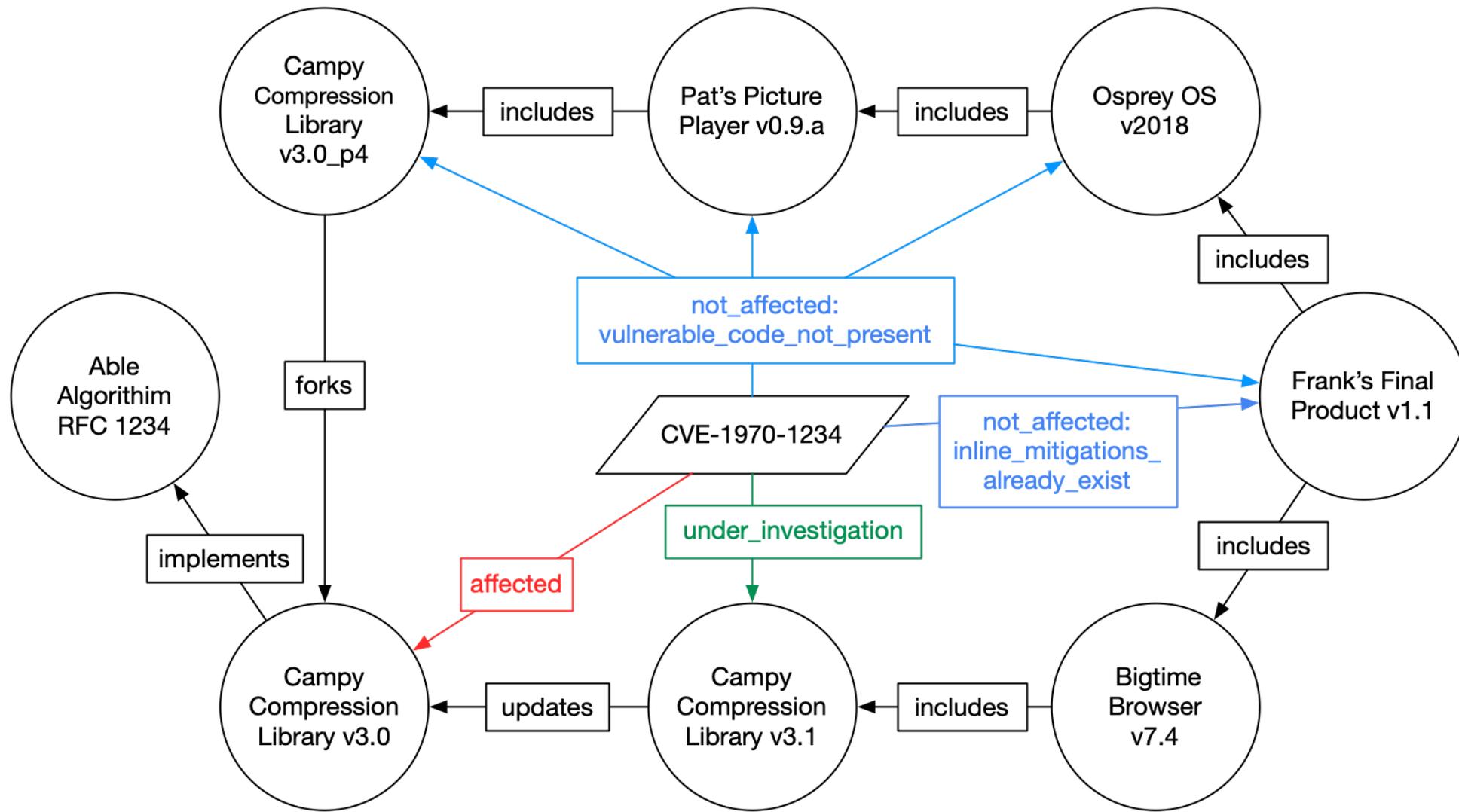












VEX publications

- Vulnerability-Exploitability eXchange (VEX) – An Overview
September 2021
- Vulnerability Exploitability eXchange (VEX) – Use Cases
April 2022
- Vulnerability Exploitability eXchange (VEX) – Status Justifications
June 2022
- Minimum Requirements for Vulnerability Exploitability eXchange (VEX)
April 2023
- When to Issue VEX Information (working title)

VEX implementations

- CSAF 2.0 Profile 5: VEX
- CycloneDX
- OpenVEX
- SPDX 3.0 Release Candidate

VEX Working Group

SBOM-a-Rama

2023-06-14

Art Manion

zmanion@protonmail.com