Tracing Vulnerabilities in Maven: A Study of CVE lifecycles and Dependency Networks

Corey Yang-Smith
corey.yangsmith@ucalgary.ca

Ahmad Abdellatif
ahmad.abdellatif@ucalgary.ca

UNIVERSITY OF
CALGARY

The Problem in Software Ecosystems

CVE-2021-44228

4% of Packages

17,000 affected

2 years later,

40% still affected

Source: https://www.cybersecuritydive.com/news/log4j-haunts-security-community/702011/

The Problem in Software Ecosystems

IBM®
Adobe
aws
vmware
F-Secure.
cisco™
BROADCOM.
okta
FORTINET®

Source: https://www.upguard.com/blog/apache-log4j-vulnerability

How quickly do maintainers respond to vulnerabilities?

RQ1: What is the **lifecycle** of vulnerabilities in Maven artifacts?

RQ1: What is the **lifecycle** of vulnerabilities in Maven artifacts?

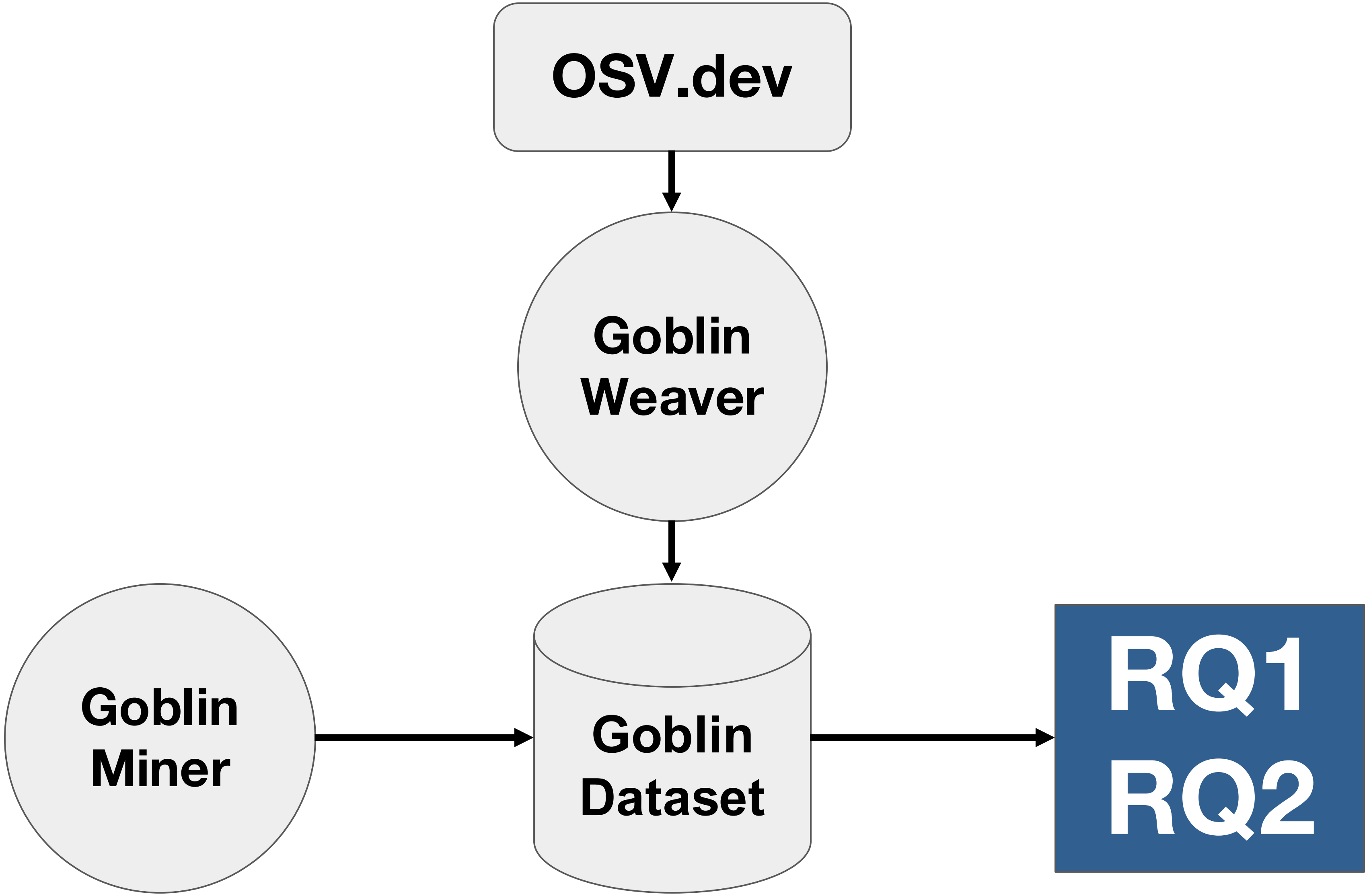
RQ2: How long does it take for **dependent packages** to adopt a new fix?

RQ1: What is the **lifecycle** of vulnerabilities in Maven artifacts?

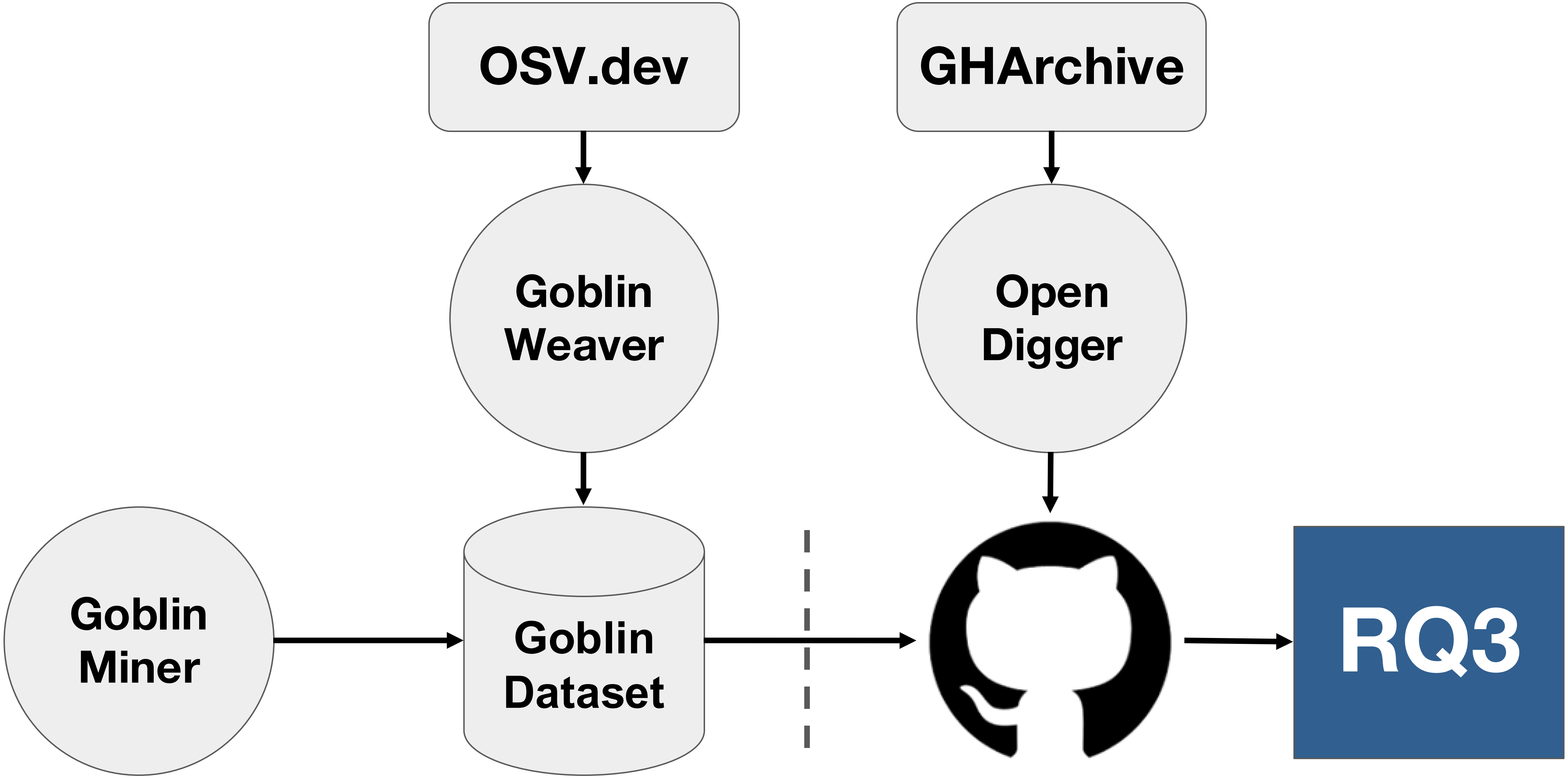
RQ2: How long does it take for **dependent packages** to adopt a new fix?

RQ3: How do **project characteristics** correlate with vulnerability outcomes?

Methodology



Methodology



RQ1: What is the **lifecycle** of vulnerabilities in Maven artifacts?

[81.6%] Patch-Before-Publish ✅

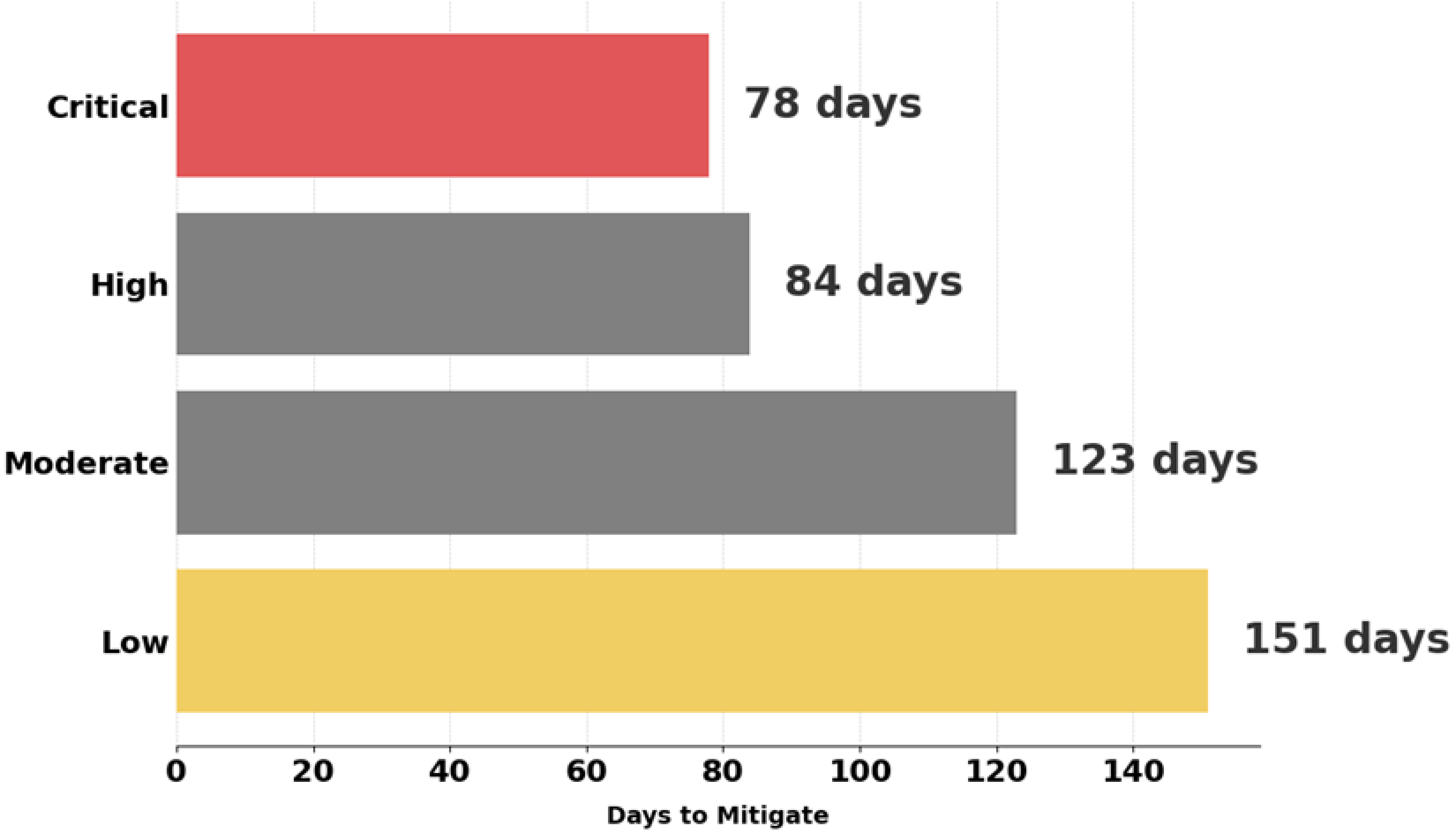
[12.8%] Publish-Before-Patch ⚠

[5.6%] Unresolved ❌

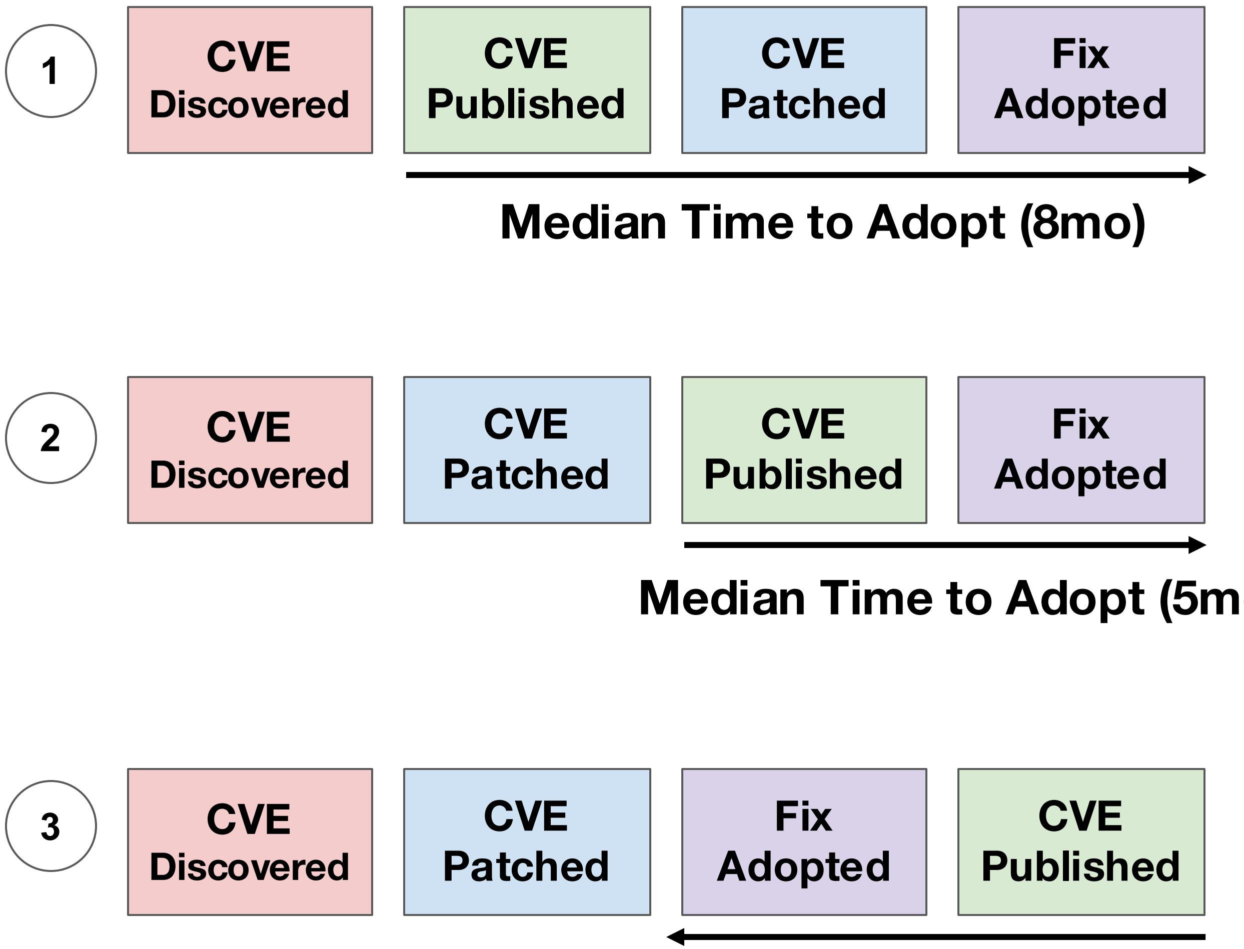
Patching often happens before disclosure - but not always.

RQ1: Maintainers **prioritize severe threats** when CVEs are disclosed.

[12.8%] Publish-Before-Patch ⚠



RQ2: How long does it take for **dependent packages** to adopt a new fix?



1 CVE Discovered → CVE Published → CVE Patched → Fix Adopted

Reactive Adoption
3,313 cases (4.5%)

Median Time to Adopt (8mo)

2 CVE Discovered → CVE Patched → CVE Published → Fix Adopted

Available Patch Adoption
46,536 cases (52.9%)

Median Time to Adopt (5mo)

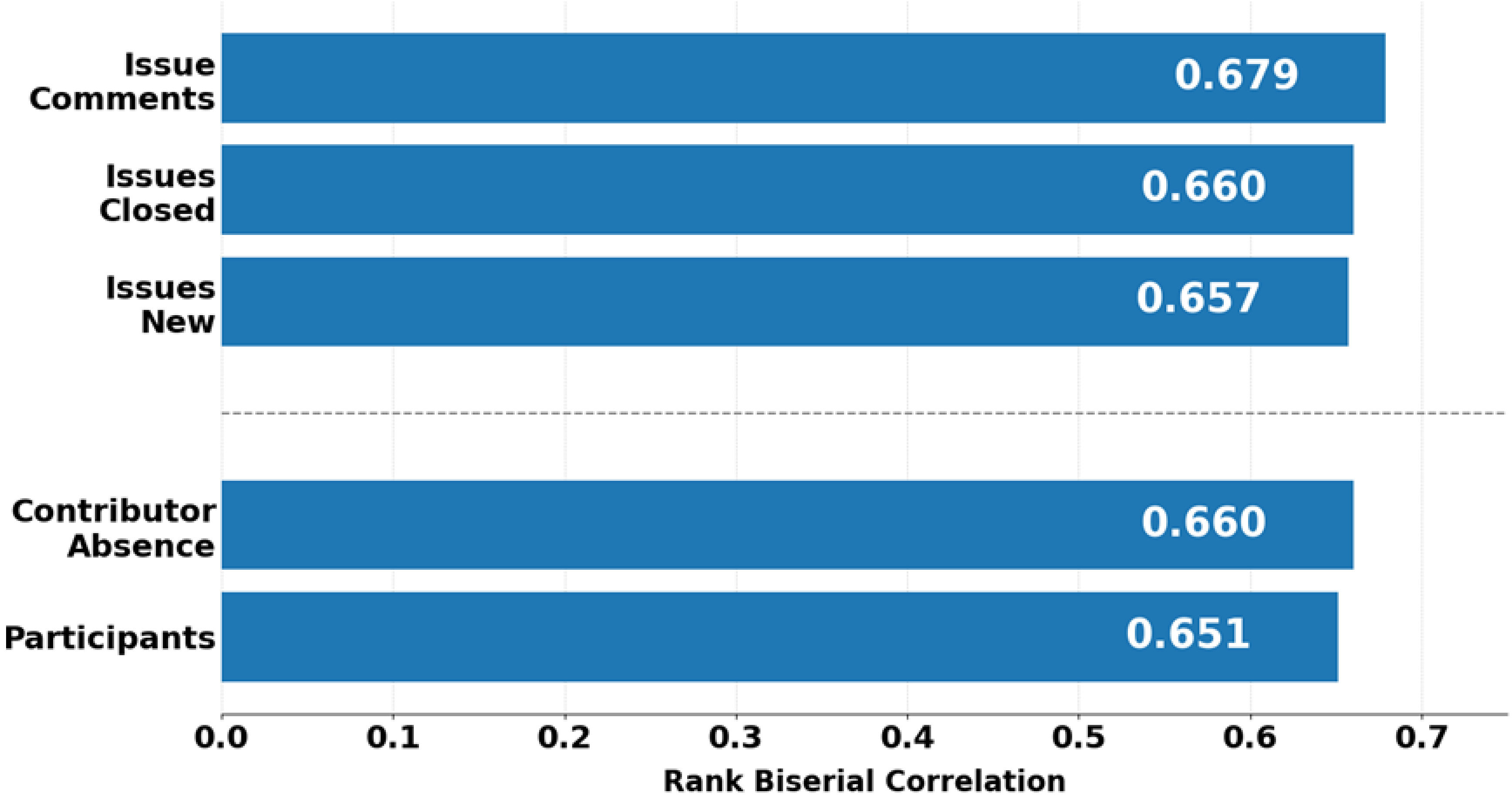
3 CVE Discovered → CVE Patched → Fix Adopted → CVE Published

Proactive Adoption
24,144 cases (32.6%)

Median Time to Adopt (11 mo)

Fixes are released quickly - but adoption still lags.

RQ3: How do **project characteristics** correlate with vulnerability outcomes?



High issue activity and contributor churn correlate with more vulnerabilities.

RQ1: What is the **lifecycle** of vulnerabilities in Maven artifacts?

[81.6%] Patch-Before-Publish ✅

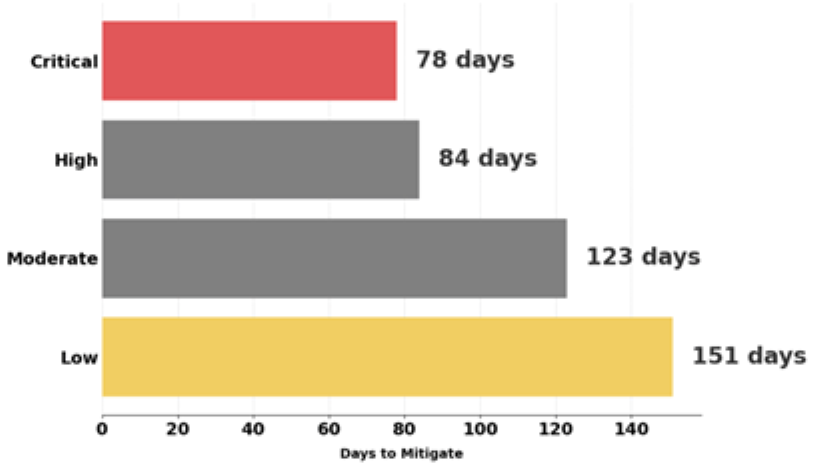
[12.8%] Publish-Before-Patch ⚠

[5.6%] Unresolved ❌

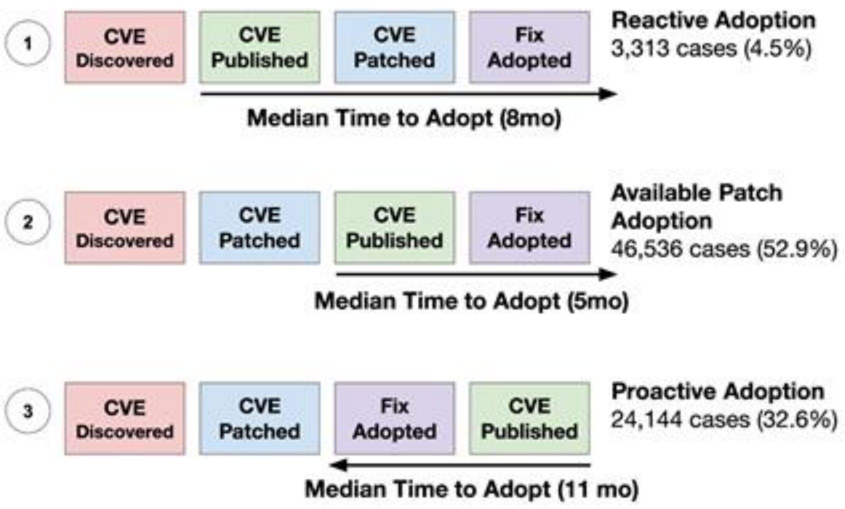
Patching often happens before disclosure - but not always.

RQ1: Maintainers **prioritize severe threats** when CVEs are disclosed.

[12.8%] Publish-Before-Patch ⚠



RQ2: How long does it take for **dependent packages** to adopt a new fix?



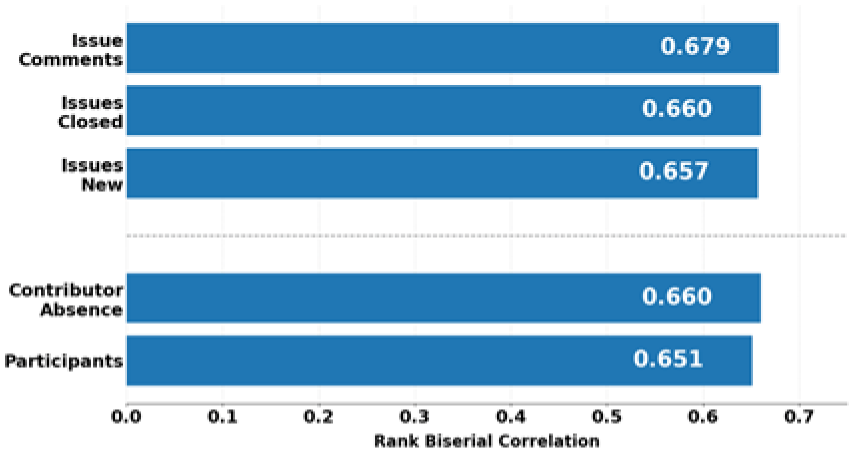
1 CVE Discovered → CVE Published → CVE Patched → Fix Adopted
Reactive Adoption
3,313 cases (4.5%)
Median Time to Adopt (8mo)

2 CVE Discovered → CVE Patched → CVE Published → Fix Adopted
Available Patch Adoption
46,536 cases (52.9%)
Median Time to Adopt (5mo)

3 CVE Discovered → CVE Patched → Fix Adopted → CVE Published
Proactive Adoption
24,144 cases (32.6%)
Median Time to Adopt (11 mo)

Fixes are released quickly - but adoption still lags.

RQ3: How do **project characteristics** correlate with vulnerability outcomes?



High issue activity and contributor churn correlate with more vulnerabilities.