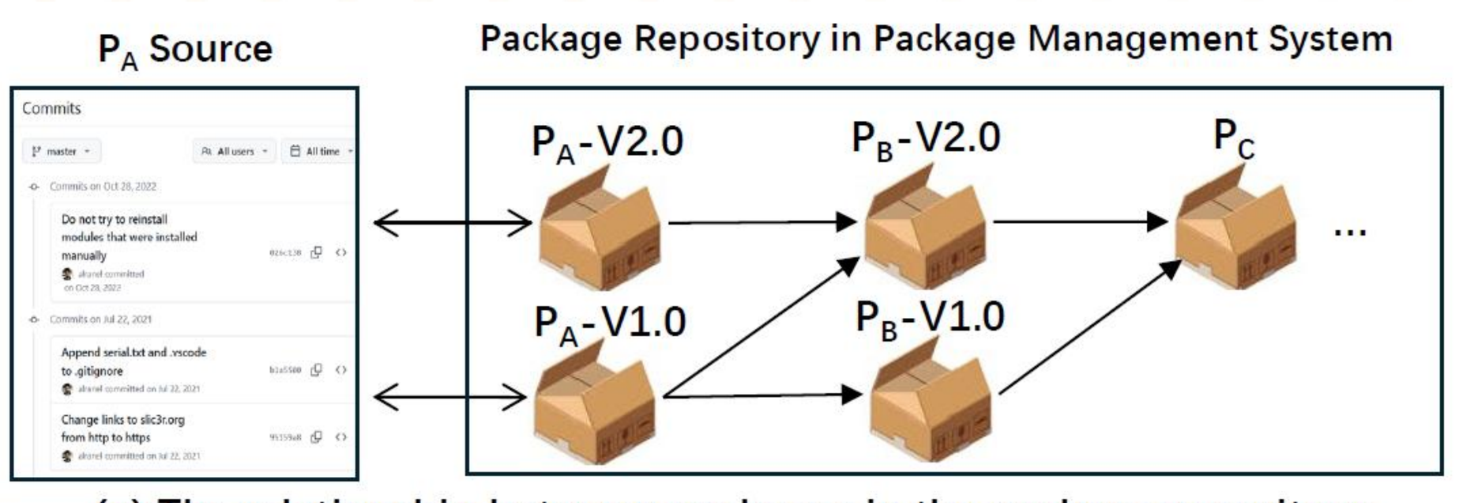
Towards Efficient C/C++ Vulnerability Impact Assessment in Package Management Systems

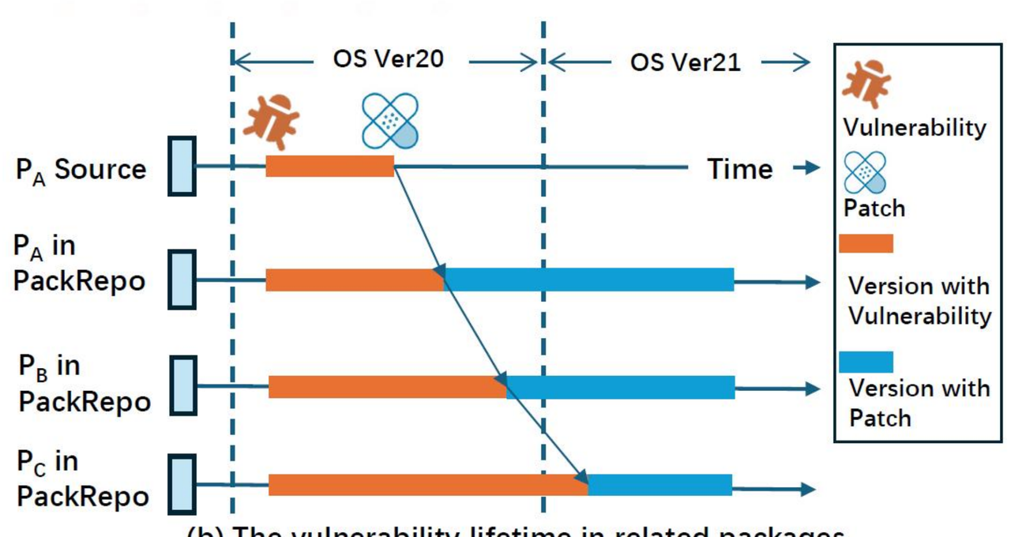
面向包管理系统的C/C++漏洞影响评估

王梓博，贾相堃，闫佳✉，杨轶，黄桦烽，苏璞睿. yanjia@iscas.ac.cn. ICICS 2025

Background



(a) The relationship between packages in the package repository.

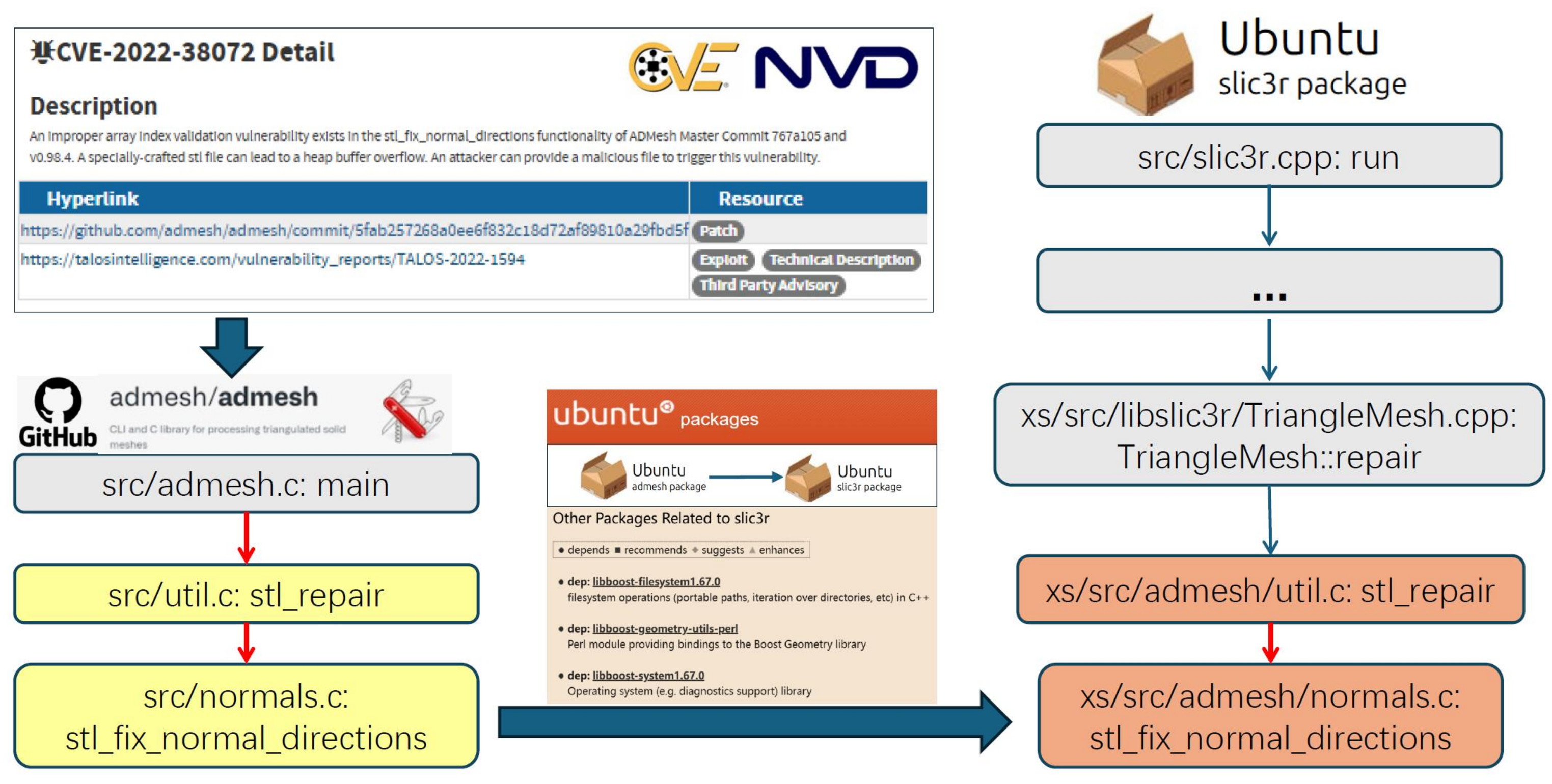


(b) The vulnerability lifetime in related packages.

(a) 包管理系统的仓库中包之间存在复杂的依赖关系，如包A在仓库中有多个版本，包B依赖A也存在多个版本

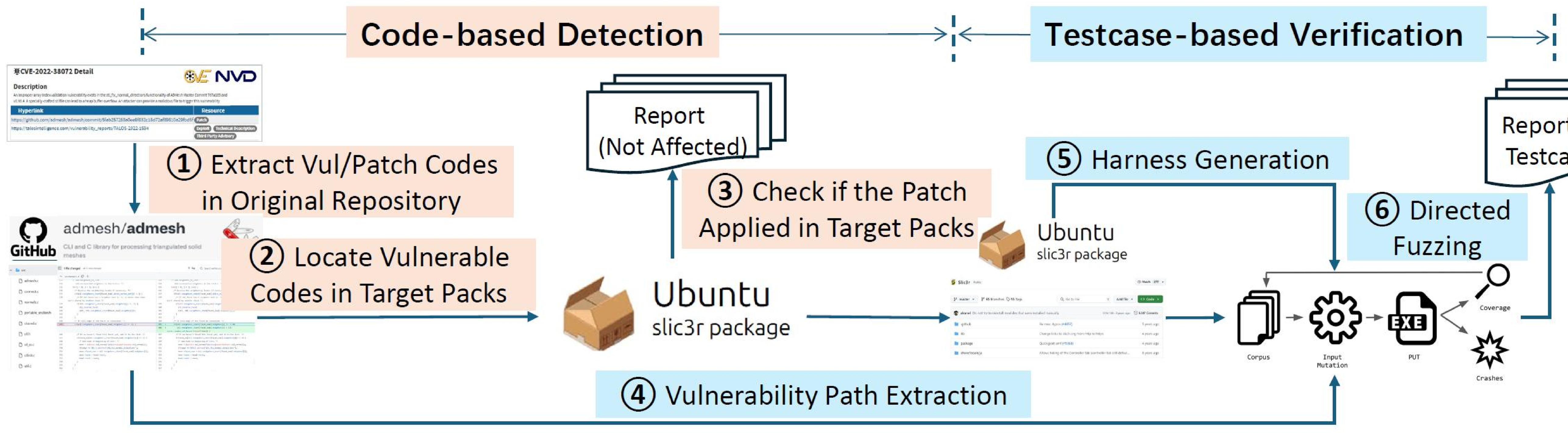
(b) 包A如果存在漏洞，会影响依赖A的包B、包C，且这种漏洞影响可能是跨越操作系统版本的

Motivation



- CVE-2022-38072是admesh的漏洞。包管理系统中存在其他依赖admesh的包（如slic3r）可能受到该漏洞影响。发现所有受到漏洞影响的包是彻底消除漏洞被使用的基础。
- version信息的丢失或不准确会导致version-based方法不可靠；code-based方法难以应对调用方式改变等情况；testcase-based方法受限于定向模糊测试等方法对复杂状态空间的探索能力。

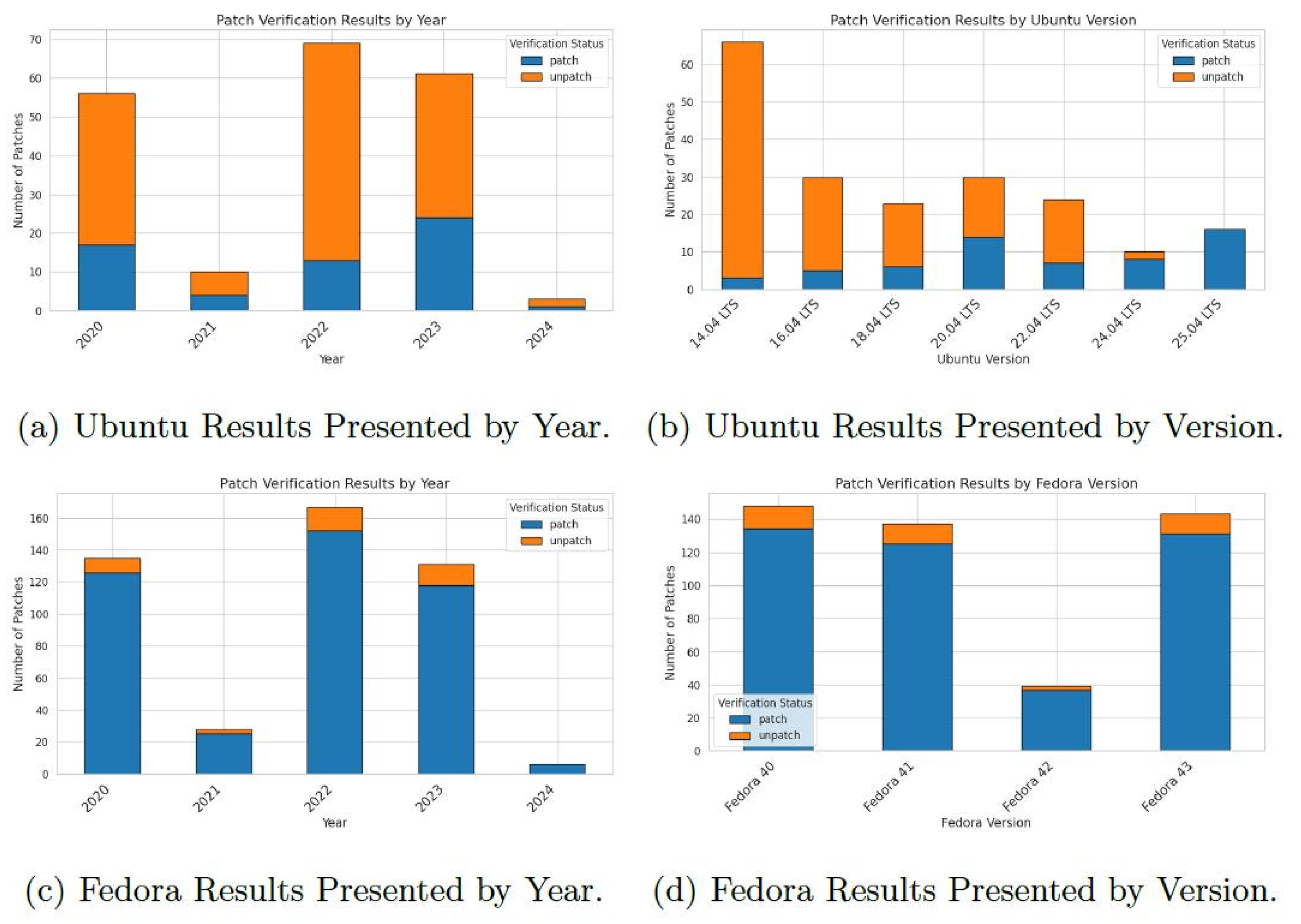
Approach



根据漏洞代码是否存在和补丁代码是否存在，code-based方法面临4种情况，其中只有“漏洞代码存在但补丁代码不存在”需要额外采用testcase-based方法验证。因此，本文提出了采用code-based detection和testcase-based verification的分阶段检测的方案，并分别对两个阶段提出了context-aware code matching和directed fuzzing on sliced harness的改进方法。

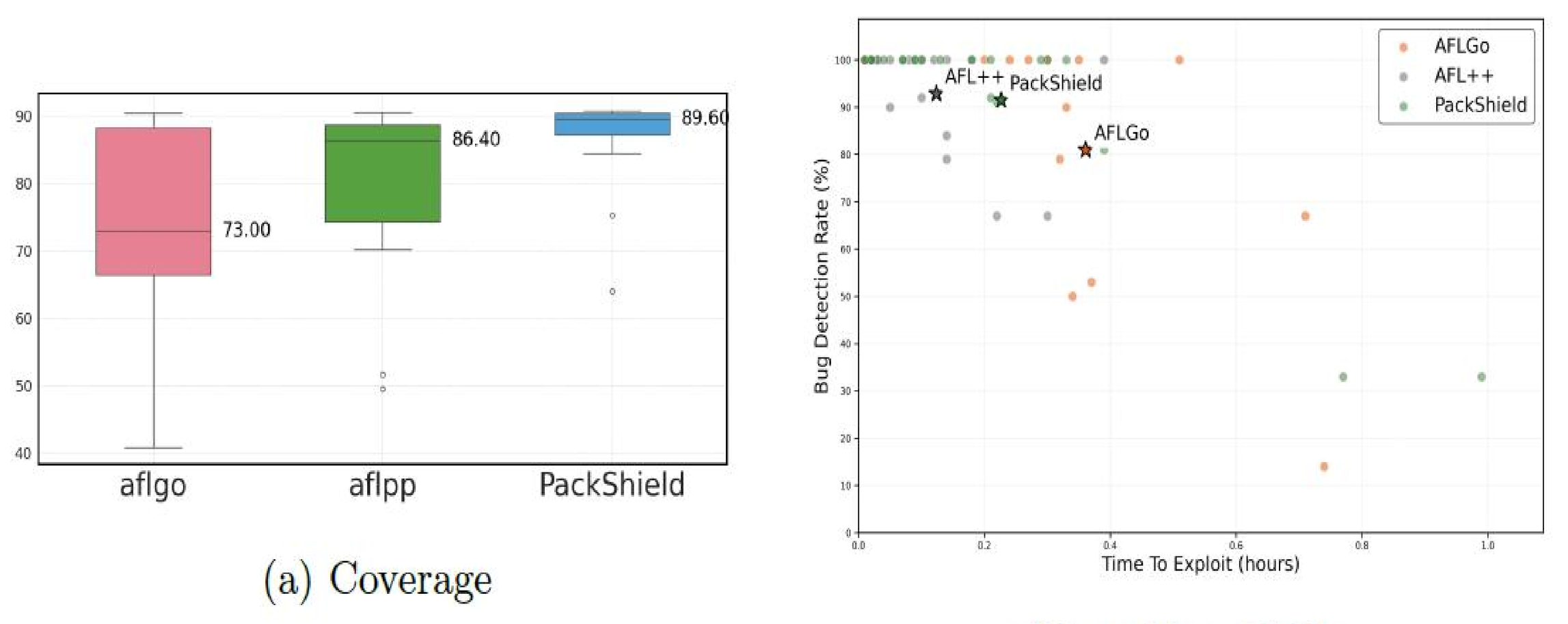
Evaluation

本文实现了PackShield，通过爬取NVD网站2020-2024的漏洞报告构建了一个包含3321个漏洞数据集。进一步应用PackShield评估了上述漏洞在两个流行软件包管理系统（Ubuntu APT系统和Fedora DNF系统）中的影响范围。实验在Ubuntu APT系统中发现存在未修复漏洞包问题345个，涉及6个Ubuntu版本；发现Fedora DNF系统存在40个问题，涉及4个Fedora版本。特别的，实验结果指出了旧操作系统版本中存在的安全问题，避免了产生官方放弃维护后不再被修复的“永久性问题”。对比实验表明PackShield相比商业解决方案OWASP Dependency-Check和论文方案V1SCAN更有效。



(a) Ubuntu Results Presented by Year. (b) Ubuntu Results Presented by Version.
(c) Fedora Results Presented by Year. (d) Fedora Results Presented by Version.

Code-based detection的结果



(a) Coverage
(b) TTE vs BDR

Directed fuzzing的对比效果

Table 1: Results of PackShield (* means 'affect multiple versions')

CVE-ID	origin repo	Package	Version	Update	OS Version	Patch	VulPath	PoC
CVE-2022-3821	systemd/systemd	ubuntu/+source/network-manager	1.48.8-1ubuntu3	2024-10-17	Ubuntu 25.04*	✓	-	-
			1.46.0-1ubuntu2	2024-04-06	Ubuntu 24.04	✓	-	-
			1.36.6-0ubuntu2	2022-06-21	Ubuntu 22.04	✓	-	-
			1.22.10-1ubuntu2.4	2024-02-26	Ubuntu 20.04	✗	✓	✗
			1.10.6-2ubuntu1.5	2023-06-02	Ubuntu 18.04	✗	✓	✗
			1.2.6-0ubuntu0.16.04.4	2019-12-06	Ubuntu 16.04	✗	✓	✗
			0.9.8.8-0ubuntu7.3	2016-05-12	Ubuntu 14.04	-	-	-
		ubuntu/+source/casync	2+20201210-2build3	2024-10-17	Ubuntu 25.04*	✗	✓	✗
			2+20201210-1build1	2021-12-09	Ubuntu 22.04	✗	✓	✗
			2+20190213-1	2019-10-18	Ubuntu 20.04	✗	✓	✗
			2+61.20180112-1	2018-02-19	Ubuntu 18.04	-	-	-
CVE-2022-3626	libtiff/libtiff	ubuntu/+source/sfftobmp	3.1.3-9build2	2024-10-17	Ubuntu 25.04*	✗	✓	✓
			3.1.3-8	2021-11-10	Ubuntu 22.04	✗	✓	✓
			3.1.3-7build1	2020-02-04	Ubuntu 20.04	✗	✓	✓
			3.1.3-5build5	2017-10-31	Ubuntu 18.04	✗	✓	✓
			3.1.3-5build1	2015-10-22	Ubuntu 16.04	✗	✓	✓
			3.1.3-3ubuntu2	2013-10-24	Ubuntu 14.04	✗	✓	✓
		ubuntu/+source/libtk-img	1:1.4.16+dfsg1-2	2024-10-17	Ubuntu 25.04*	✓	-	-
			1:1.4.16+dfsg1-1build2	2024-04-04	Ubuntu 24.04	✓	-	-
			1:1.4.13+dfsg-1	2021-10-15	Ubuntu 22.04	✗	✓	✓
			1:1.4.9+dfsg-1	2019-10-18	Ubuntu 20.04	✗	✓	✓
			1:1.4.7+dfsg-2	2018-02-05	Ubuntu 18.04	✗	✓	✓
			1:1.4.2+dfsg-2	2015-10-22	Ubuntu 16.04	✗	✓	✓
			1:1.4.2-4ubuntu1	2013-12-18	Ubuntu 14.04	✗	✓	✓
CVE-2022-39028	debian/pkgs/inetutils	ubuntu/+source/netkit-telnet	0.17-44build1	2022-04-01	Ubuntu 22.04	✗	✓	-
			0.17-41.2build1	2020-03-23	Ubuntu 20.04	✗	✓	-
			0.17-41	2017-10-24	Ubuntu 18.04	✗	✓	-
			0.17-40	2015-10-22	Ubuntu 16.04	✗	✓	-
			0.17-36build2	2013-10-18	Ubuntu 14.04	✗	✓	-
		ubuntu/+source/netkit-telnet-ssl	0.17.41+really0.17-5	2024-10-17	Ubuntu 25.04*	✗	✓	-
			0.17.41+really0.17-4build2	2024-04-04	Ubuntu 24.04	✗	✓	-
			0.17.41+0.2-3.3build2	2021-12-06	Ubuntu 22.04	✗	✓	-
			0.17.41+0.2-3.2build1	2020-03-24	Ubuntu 20.04	✗	✓	-
			0.17.41+0.2-3build1	2018-02-08	Ubuntu 18.04	✗	✓	-
			0.17.40+0.2-1	2015-10-22	Ubuntu 16.04	✗	✓	-
			0.17.24+0.1-24	2014-02-28	Ubuntu 14.04	✗	✓	-
CVE-2022-3970	libtiff/libtiff	ubuntu/+source/qt6-imageformats	6.6.2-2	2024-10-17	Ubuntu 25.04*	✓	-	-
			6.4.2-5build2	2024-04-03	Ubuntu 24.04	✗	✗	-
			6.2.4-1	2022-04-04	Ubuntu 22.04	✗	✗	-
		ubuntu/+source/qtimageformats-opensource-src	5.15.13-2	2024-10-17	Ubuntu 25.04*	✓	-	-
			5.15.13-1	2024-04-13	Ubuntu 24.04	✓	-	-
			5.15.3-1	2022-04-01	Ubuntu 22.04	✗	✗	-
			5.12.8-0ubuntu1	2020-04-14	Ubuntu 20.04	✗	✗	-
			5.9.5-0ubuntu1	2018-04-17	Ubuntu 18.04	✗	✗	-
			5.5.1-2build1	2015-12-10	Ubuntu 16.04	✗	✗	-
			5.2.1-1	2014-03-14	Ubuntu 14.04	✗	✗	-
		ubuntu/+source/libgrokj2k	10.0.5-1build4	2024-04-29	Ubuntu 24.10*	✗	✗	-
		ubuntu/+source/gdal	3.9.1+dfsg-1build2	2024-10-17	Ubuntu 25.04*	✓	-	-
			3.8.4+dfsg-3ubuntu3	2024-04-07	Ubuntu 24.04	✓	-	-
			3.4.1+dfsg-1build4	2022-03-19	Ubuntu 22.04	✗	✓	✓
			3.0.4+dfsg-1build3	2020-03-30	Ubuntu 20.04	✗	✓	✓
			2.2.3+dfsg-2	2018-02-12	Ubuntu 18.04	✗	✓	✓
			1.11.3+dfsg-3build2	2016-04-07	Ubuntu 16.04	✗	✓	✓
			1.10.1+dfsg-5ubuntu1	2014-04-05	Ubuntu 14.04	✗	✓	✓
		rpms/gdal	gdal-3.10.2-5.fc43	2025-02-27	Fedora 43	✓	-	-
			gdal-3.10.2-1.fc42	2025-02-15	Fedora 42	✓	-	-
			gdal-3.9.3-1.fc41	2024-10-15	Fedora 41	✓	-	-
			gdal-3.8.5-2.fc40	2024-04-14	Fedora 40	✓	-	-
CVE-2022-38072	admesh/admesh	ubuntu/+source/slic3r	1.3.0+dfsg1-5build6	2024-04-29	Ubuntu 24.10*	✗	✓	✓
			1.3.0+dfsg1-5build1	2022-03-02	Ubuntu 22.04	✗	✓	✓
			1.3.0+dfsg1-3ubuntu1	2020-02-09	Ubuntu 20.04	✗	✓	✓
			1.2.9+dfsg-9	2018-02-02	Ubuntu 18.04	✗	✓	✓
			1.2.9+dfsg-2build1	2016-01-06	Ubuntu 16.04	✗	✓	✓
		rpms/slic3r	slic3r-1.3.0-47.fc42	2025-01-19	Fedora 43*	✗	✓	✓
			slic3r-1.3.0-45.fc41	2024-07-21	Fedora 41	✗	✓	✓
			slic3r-1.3.0-33.fc40	2024-01-27	Fedora 40	✗	✓	✓
CVE-2023-0798	libtiff/libtiff	ubuntu/+source/libtk-img	1:1.4.16+dfsg1-2	2024-10-17	Ubuntu 25.04*	✗	✓	✓
			1:1.4.16+dfsg1-1build2	2024-04-04	Ubuntu 24.04	✗	✓	✓
			1:1.4.13+dfsg-1	2021-10-15	Ubuntu 22.04	✗	✓	✓
			1:1.4.9+dfsg-1	2019-10-18	Ubuntu 20.04	✗	✓	✓
			1:1.4.7+dfsg-2	2018-02-05	Ubuntu 18.04	✗	✓	✓
			1:1.4.2+dfsg-2	2015-10-22	Ubuntu 16.04	✗	✓	✓
			1:1.4.2-4ubuntu1	2013-12-18	Ubuntu 14.04	✗	✓	✓

漏洞影响评估结果

Table 2: Comparison results (X/Y of V1SCAN means 'target/findings')

CVE-ID	Package	Version	Affected	PackShield	Dependency-Check	V1SCAN
CVE-2022-3821	network-manager	1.48.8-1ubuntu3	✗	✗	-	-
		1.46.0-1ubuntu2	✗	✗	-	-
		1.36.6-0ubuntu2	✗	✗	-	-
		1.22.10-1ubuntu2.4	✗	✗	-	0 / 1
		1.10.6-2ubuntu1.5	✗	✗	-	0 / 1
		1.2.6-0ubuntu0.16.04.4	✗	✗	-	0 / 1
		0.9.8.8-0ubuntu7.3	✗	✗	-	0 / 1
	casync	2+20201210-2build3	✗	✗	-	-
		2+20201210-1build1	✗	✗	-	-
		2+20190213-1	✗	✗	-	-
		2+61.20180112-1	✗	✗	-	-
CVE-2022-3626	sfftobmp	3.1.3-9build2	✓	✓	-	0 / 5
		3.1.3-8	✓	✓	-	0 / 8
		3.1.3-7build1	✓	✓	-	0 / 8
		3.1.3-5build5	✓	✓	-	0 / 6
		3.1.3-5build1	✓	✓	-	0 / 6
		3.1.3-3ubuntu2	✓	✓	-	0 / 6
	libtk-img	1:1.4.16+dfsg1-2	✗	✗	-	0 /1
		1:1.4.16+dfsg1-1build2	✗	✗	-	0 / 1
		1:1.4.13+dfsg-1	✓	✓	-	0 / 3
		1:1.4.9+dfsg-1	✓	✓	-	0 / 6
		1:1.4.7+dfsg-2	✓	✓	-	0 / 6
		1:1.4.2+dfsg-2	✓	✓	-	0 / 6
		1:1.4.2-4ubuntu1	✓	✓	-	0 / 6
CVE-2022-39028	netkit-telnet	0.17-44build1	✗	✗	-	-
		0.17-41.2build1	✗	✗	-	-
		0.17-41	✗	✗	-	-
		0.17-40	✗	✗	-	-
		0.17-36build2	✗	✗	-	-
	netkit-telnet-ssl	0.17.41+really0.17-5	✗	✗	-	-
		0.17.41+really0.17-4build2	✗	✗	-	-
		0.17.41+0.2-3.3build2	✗	✗	-	-
		0.17.41+0.2-3.2build1	✗	✗	-	-
		0.17.41+0.2-3build1	✗	✗	-	-
		0.17.40+0.2-1	✗	✗	-	-
		0.17.24+0.1-24	✗	✗	-	-
CVE-2022-3970	qt6-imageformats	6.6.2-2	✗	✗	-	-
		6.4.2-5build2	✗	✗	-	-
		6.2.4-1	✗	✗	-	-
	qtimageformats-opensource-src	5.15.13-2	✗	✗	-	-
		5.15.13-1	✗	✗	-	-
		5.15.3-1	✗	✗	-	0 / 3
		5.12.8-0ubuntu1	✗	✗	-	0 / 3
		5.9.5-0ubuntu1	✗	✗	-	0 / 5
		5.5.1-2build1	✗	✗	-	0 / 7
		5.2.1-1	✗	✗	-	0 / 7
	libgrokj2k	10.0.5-1build4	✗	✗	-	-
	gdal	3.9.1+dfsg-1build2	✗	✗	-	-
		3.8.4+dfsg-3ubuntu3	✗	✗	-	-
		3.4.1+dfsg-1build4	✓	✓	-	-
		3.0.4+dfsg-1build3	✓	✓	-	0 / 1
		2.2.3+dfsg-2	✓	✓	-	0 / 3
		1.11.3+dfsg-3build2	✓	✓	-	0 / 6
		1.10.1+dfsg-5ubuntu1	✓	✓	-	0 / 7
		gdal-3.10.2-5.fc43	✗	✗	-	-
		gdal-3.10.2-1.fc42	✗	✗	-	-
		gdal-3.9.3-1.fc41	✗	✗	-	-
		gdal-3.8.5-2.fc40	✗	✗	-	-
CVE-2022-38072	slic3r	1.3.0+dfsg1-5build6	✓	✓	-	-
		1.3.0+dfsg1-5build1	✓	✓	-	-
		1.3.0+dfsg1-3ubuntu1	✓	✓	-	-
		1.2.9+dfsg-9	✓	✓	-	-
		1.2.9+dfsg-2build1	✓	✓	-	-
		slic3r-1.3.0-47.fc42	✓	✓	-	-
		slic3r-1.3.0-45.fc41	✓	✓	-	-
		slic3r-1.3.0-33.fc40	✓	✓	-	-

对比实验结果