Xray On-Demand Binary Scan

Overview

As an organization, you wish to build software securely during development, without trying to find and fix vulnerabilities after your code is compiled. Xray uses the JFrog CLI to provide on-demand binary scanning to address your needs.

- Run ad-hoc scans for security purposes without uploading to Artficatory first.
- Adhere to organizational standards, whereas binaries and builds need to be approved first before uploading to Artifactory.
- Not all binaries are stored in Artifactory, and as a user, you want to use Xray scanning capabilities.

You can point to a binary in your local file system and receive a report that contains a list of vulnerabilities and licenses for that binary. The JFrog CLI encapsulates a closed source component that contains the logic of extracting a binary and composes a component graph from the binary, similar to the way Xray scans your binaries in Artifactory. For more information, see Xray Security and Compliance. Th e CLI returns a detailed scan results report that contains the details of vulnerabilities, violations, and licenses discovered in your binary.

> Starting from Xray version 3.40.3 and JFrog CLI version 2.11.0, you can run an on-demand binary scan on Docker images.

Page Contents

Setting Up On-Demand Binary Scan

1. Install Xray
2. Install JFrog CLI version 2.1.0

How Does it Work?

Step 1 - Trigger the JFrog CLI

Trigger the JFrog CLI in a directory containing the binaries of a project.

Step 2 - Run the JFrog CLI Commands

Run the JFrog CLI Commands using one of the two methods:

- Use the existing upload command with additional parameters that will serve as a conditional upload. A conditional upload ensures that the files are scanned prior to uploading to Artifactory, and will not be uploaded if the scan contains any security issues and does not comply with the policies you set.
- Run an independent scan command.

Supported commands in the JFrog CLI:

- Scanning Files on the Local File System: This command scans files on the local file-system with Xray.

Depending on the command option you use, you can view scan results for the following:

- Vulnerabilities
- Violations
- Licenses

By default, the scan returns vulnerabilities data found in your dependencies. To retrieve violations data, use one of the following methods:

- **Watches -** Select Watches to apply to the scan.
- **Repo Path** - Provide a target destination path in Artifactory, and Watches will be determined by the path.
- **Project** - Select a Project by project key, and use all Watches defined for the Project.

Take note, that if you run the scan using one of these command options, the scan results will only show violations data and not vulnerabilities data. To view vulnerabilities data, run the scan without these options.

Step 3 - View Results

The results are displayed in table format.

Security Violations

SEVERITY	IMPACTED PACKAGE	IMPACTED PACKAGE VERSION	TYPE	FIXED VERSIONS	COMPONENT	COMPONENT VERSION	CVE	CVSS V2	CVSS V3	ISSUE ID
Critical	commons-io:commons-io	2.6	Maven	[2.7]	commons-io:commons-io	2.6		5.0		XRAY-78200
High	commons-io:commons-io	2.6	Maven	[2.8.0]	commons-io:commons-io	2.6		7.1	7.5	XRAY-125253
Medium	org.apache.httpcomponents :httpclient	4.5.6	Maven	[4.5.13]	org.apache.httpcomponents :httpclient	4.5.6	CVE-2020-13956	5.0	5.3	XRAY-129495
Medium	commons-io:commons-io	2.6	Maven	[2.7]	commons-io:commons-io	2.6	CVE-2021-29425	5.0	5.3	XRAY-172728
Medium	commons-codec:commons-cod ec	1.10	Maven	[1.13]	commons-codec:commons-cod ec	1.10		5.0		XRAY-87486
Medium	org.postgresql:postgresql	42.2.0	Maven	[42.2.13]	org.postgresql:postgresql	42.2.0	CVE-2020-13692	6.8	7.7	XRAY-146611
Medium	org.postgresql:postgresql	42.2.0	Maven	[42.2.5]	org.postgresql:postgresql	42.2.0	CVE-2018-10936	6.8	8.1	XRAY-77885
Medium	log4j:log4j	1.2.17	Maven		log4j:log4j	1.2.17	CVE-2020-9488	4.3	3.7	XRAY-96751
Low	log4j:log4j	1.2.17	Maven		log4j:log4j	1.2.17		6.9		XRAY-87321

License Compliance Violations

LICENSE	SEVERITY	IMPACTED PACKAGE	IMPACTED PACKAGE VERSION	TYPE	COMPONENT	COMPONENT VERSION
BSD 2-Clause	High	com.ongres.scram:common	1.0.0-beta.2	Maven	com.ongres.scram:common	1.0.0-beta.2
BSD 2-Clause	High	org.postgresql:postgresql	42.2.0	Maven	org.postgresql:postgresql	42.2.0

You can also view results in JSON format for automation purposes and view more scan results data by using the following command option:

```
--format=json
```

Sample Output


```
{
  "scan_id": "11148acb-f8d4-4640-56e4-db312cb5ba0c",
  "violations": [
    {
      "summary": "Apache Commons IO FileNameUtils.normalize Path Traversal Remote File Disclosure Weakness",
      "severity": "Medium",
      "type": "security",
      "components": {
        "gav://commons-io:commons-io:2.2": {
          "fixed_versions": [
            "[2.7]"
          ],
          "impact_paths": [
            [
              {
                "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
              },
              {
                "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
              },
              {
                "component_id": "gav://commons-io:commons-io:2.2",
                "full_path": "META-INF/maven/commons-io/commons-io/pom.xml"
              }
            ]
          ]
        }
      },
      "watch_name": "Sec-Watch",
      "issue_id": "XRAY-78200",
```

```
      "ignore_url": "http://jfrog.com/ui/admin/xray/policiesGovernance/ignore-rules?graph_scan_id=11148acb-
f8d4-4640-56e4-db312cb5ba0c&issue_id=XRAY-78200&show_popup=true&type=security&watch_name=Sec-Watch",
      "cves": [
        {
        }
      ],
      "references": [
        "https://issues.apache.org/jira/browse/IO-556"
      ],
    },
    {
      "severity": "Medium",
      "type": "security",
      "components": {
        "gav://commons-io:commons-io:2.2": {
          "fixed_versions": [
            "[2.7]"
          ],
          "impact_paths": [
            [
              {
                "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
              },
              {
                "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
              },
              {
                "component_id": "gav://commons-io:commons-io:2.2",
                "full_path": "META-INF/maven/commons-io/commons-io/pom.xml"
              }
            ]
          },
          "watch_name": "Sec-Watch",
          "issue_id": "XRAY-172728",
          "ignore_url": "http://jfrog.com/ui/admin/xray/policiesGovernance/ignore-rules?
graph_scan_id=11148acb-f8d4-4640-56e4-db312cb5ba0c&issue_id=XRAY-
172728&show_popup=true&type=security&watch_name=Sec-Watch",
          "cves": [
            {
              "cve": "CVE-2021-29425",
              "cvss_v2_score": "5.0",
              "cvss_v2_vector": "CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:N",
              "cvss_v3_score": "5.3",
              "cvss_v3_vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N"
            }
          ],
          "references": [
            "https://issues.apache.org/jira/browse/IO-556",
            "https://lists.apache.org/thread.html/rc359823b5500e9a9a2572678ddb8e01d3505a7ffcadfa8d13b8780ab%
40%3Cuser.commons.apache.org%3E"
          ],
        },
        {
          "severity": "High",
          "type": "license",
          "components": {
            "gav://org.slf4j:slf4j-api:1.7.5": {
              "impact_paths": [
                [
                  {
                    "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                  },
                  {
                    "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                    "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                  },
                  {
                    "component_id": "gav://org.slf4j:slf4j-api:1.7.5",
                    "full_path": "META-INF/maven/org.slf4j/slf4j-api/pom.xml"
                  }
```

```
              ]
            ]
          }
        },
        "watch_name": "Sec-Watch",
        "ignore_url": "http://jfrog.com/ui/admin/xray/policiesGovernance/ignore-rules?
graph_scan_id=11148acb-f8d4-4640-56e4-db312cb5ba0c&issue_id=MIT&show_popup=true&type=security&watch_name=Sec-
Watch",
        "references": [
          "http://www.opensource.org/licenses/MIT",
          "http://www.opensource.org/licenses/mit-license.php",
          "https://spdx.org/licenses/MIT",
          "https://spdx.org/licenses/MIT.html"
        ],
        "license_key": "MIT",
        "license_name": "The MIT License",
      }
    ],
    "licenses": [
      {
        "license_key": "Apache-2.0",
        "components": {
          "gav://commons-io:commons-io:2.2": {
            "impact_paths": [
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                },
                {
                  "component_id": "gav://commons-io:commons-io:2.2",
                  "full_path": "META-INF/maven/commons-io/commons-io/pom.xml"
                }
              ]
            ]
          },
          "gav://commons-lang:commons-lang:2.6": {
            "impact_paths": [
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                },
                {
                  "component_id": "gav://commons-lang:commons-lang:2.6",
                  "full_path": "META-INF/maven/commons-lang/commons-lang/pom.xml"
                }
              ]
            ]
          },
          "gav://de.is24.common:appmon4j-agent:1.53": {
            "impact_paths": [
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "META-INF/maven/de.is24.common/appmon4j-agent/pom.xml"
                }
              ],
```

```
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                }
              ],
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                }
              ]
            ]
          },
          "gav://de.is24.common:appmon4j-core:1.53": {
            "impact_paths": [
              [
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                },
                {
                  "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                },
                {
                }"http://www.opensource.org/licenses/Apache-2.0",
                {
                  "impact_paths": [
                  ]"status": "completed""violations": [
                    "severity": "Medium",
                    "type": "security",
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                    ],
                  },
                  "type": "security",
                  "components": {
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                      "cvss_v2_vector": "CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:N",
                    }"https://lists.apache.org/thread.html
/rc359823b5500e9a9a2572678ddb8e01d3505a7ffcadfa8d13b8780ab%40%3Cuser.commons.apache.org%3E"
                  ],
                },
                {
                },
                {
                  "references": [
                    "https://spdx.org/licenses/MIT.html""license_name": "The MIT License",
                  }"gav://commons-io:commons-io:2.2": {
                  },
                  "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar""
impact_paths": [
                    "component_id": "gav://de.is24.common:appmon4j-agent:1.53""full_path": "./usr/lib
/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                  },
                  "gav://de.is24.common:appmon4j-agent:1.53": {
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                    },
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53"[
                        {
                          "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                          [
                            {
                              "component_id": "gav://de.is24.common:appmon4j-core:1.53",
                              "full_path": "META-INF/maven/de.is24.common/appmon4j-core/pom.xml"
```

```
                    }
                  ]
                ]
              }
            },
            "references": [
              "http://www.opensource.org/licenses/Apache-2.0",
              "http://www.opensource.org/licenses/apache2.0.php",
              "https://spdx.org/licenses/Apache-2.0",
              "https://spdx.org/licenses/Apache-2.0.html",
              "http://www.apache.org/licenses/LICENSE-2.0",
              "https://licenses.nuget.org/Apache-2.0",
              "http://licenses.nuget.org/Apache-2.0",
              "https://raw.githubusercontent.com/aspnet/AspNetCore/2.0.0/LICENSE.txt",
              "http://raw.githubusercontent.com/aspnet/AspNetCore/2.0.0/LICENSE.txt"
            ]
          },
          {
            "license_key": "MIT",
            "components": {
              "gav://org.slf4j:slf4j-api:1.7.5": {
                "impact_paths": [
                  [
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53"
                    },
                    {
                      "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
                      "full_path": "./usr/lib/appmon4j/appmon4j-agent-jar-with-dependencies.jar"
                    },
                    {
                      "component_id": "gav://org.slf4j:slf4j-api:1.7.5",
                      "full_path": "META-INF/maven/org.slf4j/slf4j-api/pom.xml"
                    }
                  ]
                ]
              }
            },
            "references": [
              "http://www.opensource.org/licenses/MIT",
              "http://www.opensource.org/licenses/mit-license.php",
              "https://spdx.org/licenses/MIT",
              "https://spdx.org/licenses/MIT.html"
            ]
          }
        ],
        "component_id": "gav://de.is24.common:appmon4j-agent:1.53",
        "package_type": "Maven",
        "status": "completed"
      }
    }
```

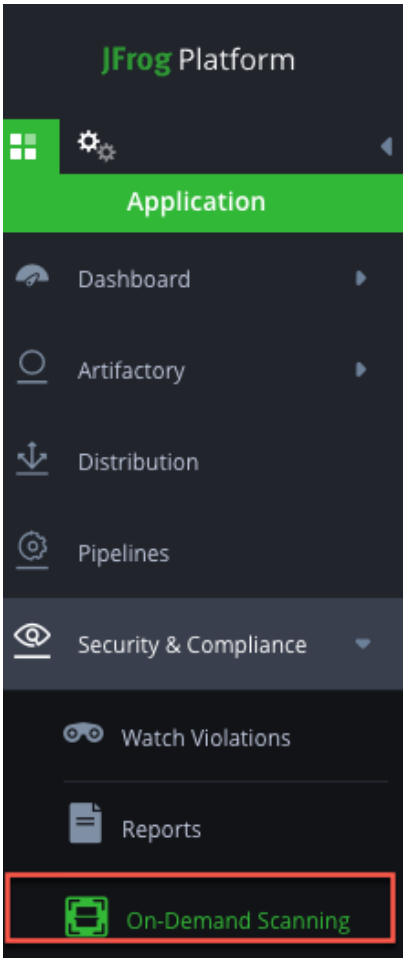

Field Name	Description	Example
artifact_name	The name of the artifact.	jenkins-war-2.289.1.war
component_id	Component ID in the JFrog Component Format Standards.	gav://org.jenkins-ci.main:jenkins-war:2.289.1
package_type	Type of the artifact package.	Maven
repo_path	The repo path as it was provided in the scan request.	default/maven-local-repo/org/jenkins-ci/main/jenkins-war/2.289.1/
scan_id	Unique scan ID.	4f811ab8-51a2-4baf-61d3-3a277aaa8066
status	Scan status. If a scan is pending, completed or failed.	pending failed completed

violations	A list of minimal violations.	
violations[].summary		
violations[].severity		Medium Critical
violations[].type	Security or license.	security
violations[].components	Map of violating component the lowest level in the artifact graph. The key is the component ID.	
violations[].components[].impact_paths	List of impact paths. Each impact path is a JSON array by itself, indicating the path from the artifact in scan to the vulnerable component in the graph.	
violations[].components[].impact_paths[][].component_id	The component ID in the current impact path node.	gav://commons-httpclient:commons-httpclient:3.1-jenkins-2
violations[].components[].impact_paths[][].full_path	The file path of the current component, relative to the previous component in the list. The first component (which is the artifact itself) will not have full_path filled.	META-INF/maven/commons-httpclient/commons-httpclient/pom.xml
violations[].components[].fixed_versions	Versions of the component in which this violation is not effective anymore.	["[4.0.9-2+deb9u4]", "[4.0.10-3+deb9u4]"]
violations[].watch_name	Watch that created the violation.	cloud-watch
violations[].issue_id	Xray issue ID.	XRAY-73704
violations[].ignore_url	Violation Ignore Rule Creation URL.	http://jfrog.com/ui/admin/xray/policiesGovernance/ignore-rules?graph_scan_id=11148acb-f8d4-4640-56e4-db312cb5ba0c&issue_id=MIT&show_popup=true&type=security&watch_name=Sec-Watch
violations[].cves	List of CVE objects.	
violations[].cves[].cve	CVE ID.	CVE-2018-9116
violations[].cves[].cvss_v2_score		6.4
violations[].cves[].cvss_v3_score		9.1
violations[].cves[].cvss_v2_vector		CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:P
violations[].cves[].cvss_v3_vector		CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
violations[].references	Links for more information.	
violations[].fail_build	Indicates if this violation fails a build.	true
violations[].license_key		Apache-2.0
violations[].license_name		The Apache Software License, Version 2.0
vulnerabilities	List of vulnerabilities discovered on the scanned graph.	
vulnerabilities[].cves	List of CVE objects.	
vulnerabilities[].summary	Summary of the vulnerability.	

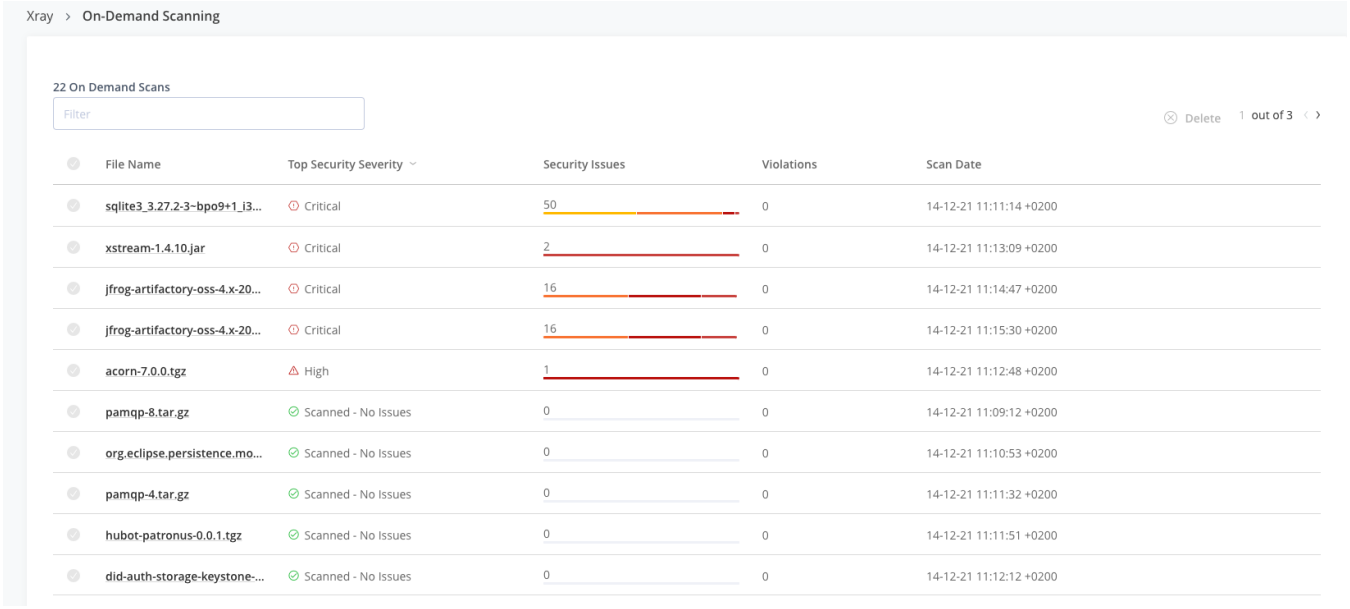
vulnerabilities[].severity		Medium Critical
vulnerabilities[].vulnerable_components	List of vulnerable components the lowest level in the artifact graph	["npm://highlight.js:9.18.3"]
vulnerabilities[].components	List of vulnerable components the lowest level in the artifact graph.	
licenses	List of licenses	
licenses[].license_key		Apache-2.0
licenses[].license_name		The Apache Software License, Version 2.0
licenses[].components	Map of components with this license, where the key is component ID.	
licenses[].custom	Indicated if this is this a custom license.	false
licenses[].references	Links for more information	

View Results in the JFrog Platform

Navigate to **Administration | Security and Compliance | On-Demand Scanning**.

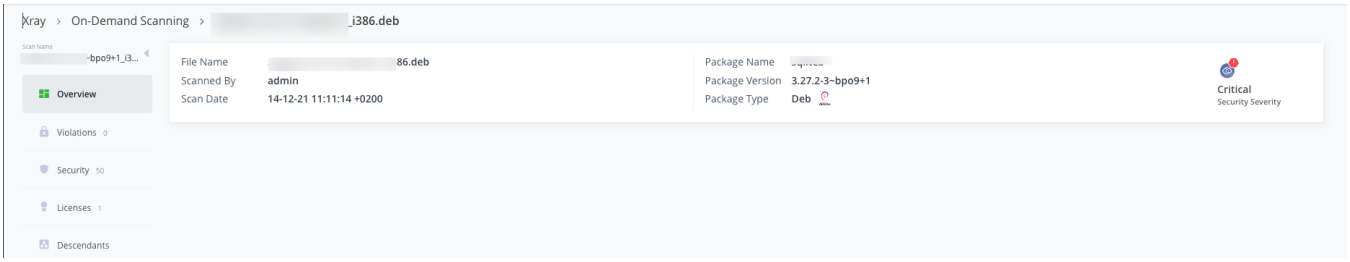


A list with all the on-demand binaries scans is displayed.

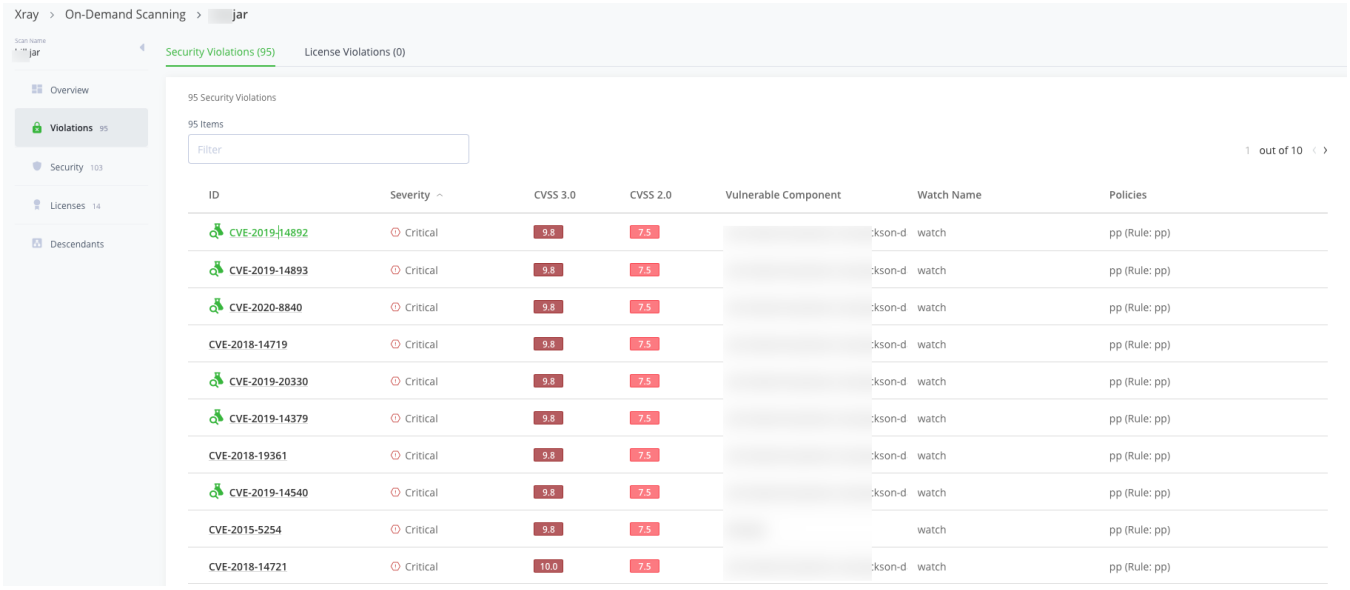


Click on a scan from the list to view the results. The results consist of a scan overview details, list of security and license violations, security vulnerabilities, discovered licenses, and descendants. You can learn more about these Xray scan results in Analyzing Resource Scan Results.

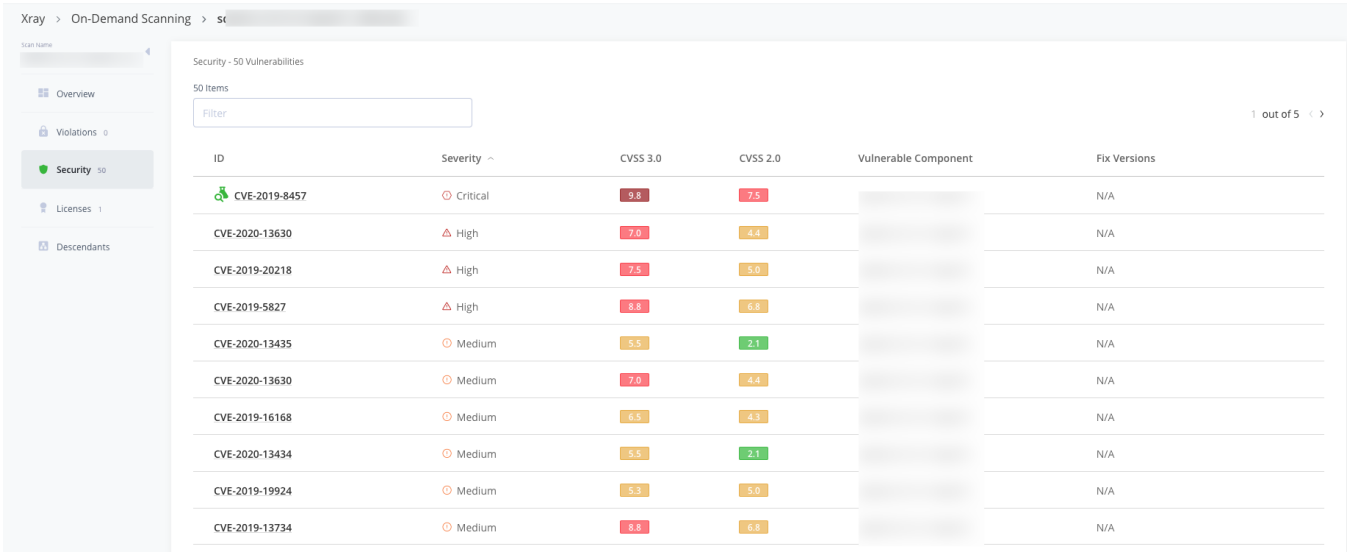
Overview



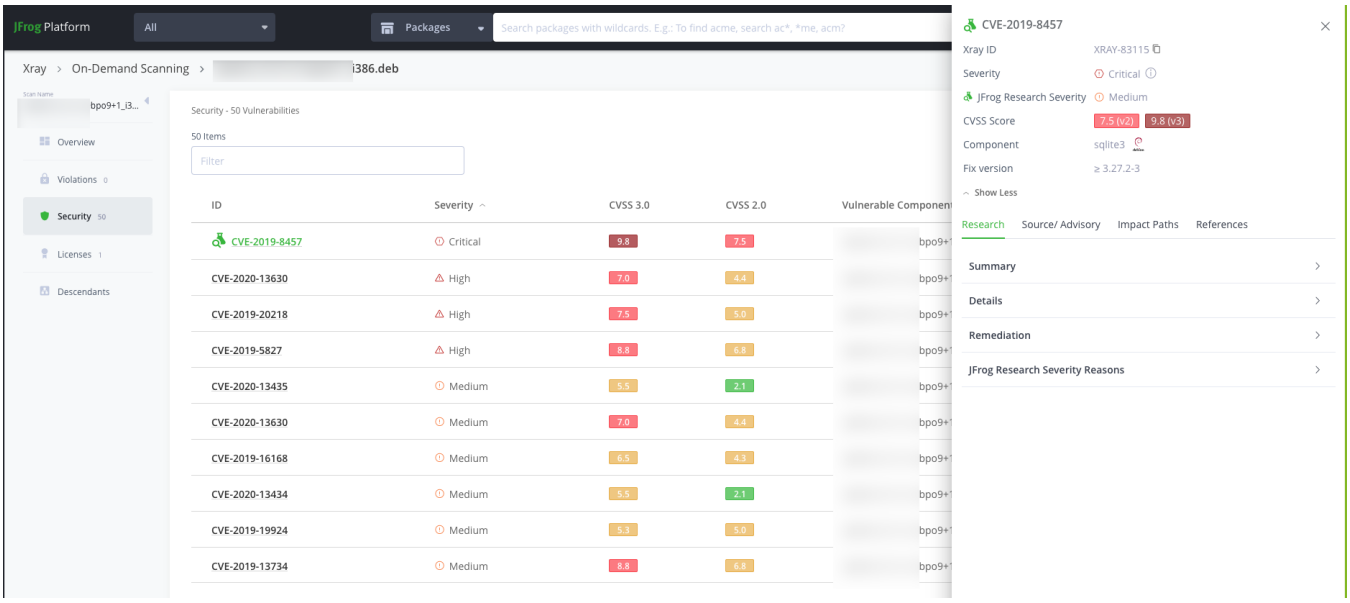
Violations



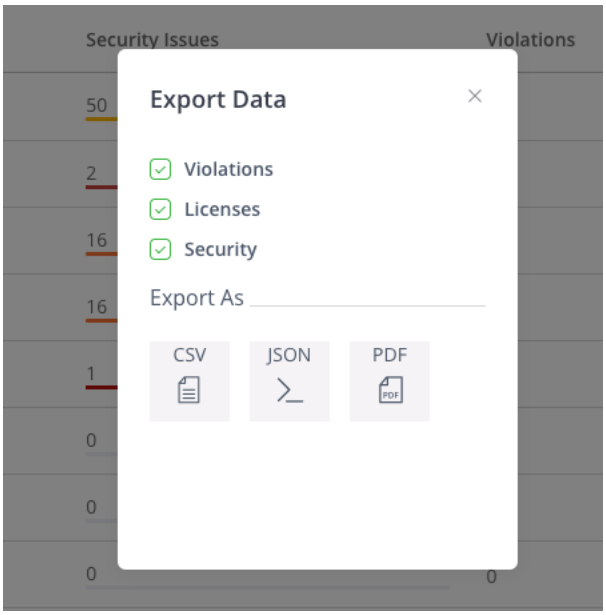
Security Vulnerabilities



CVE Details



You can also export the scan results to CSV, PDF, and JSON formats by clicking on the action icon in the scan list.



Known Limitations

- Java scripts which are not part of an npm package will not be identified in this scan. Once uploaded to Artifactory it will be fully detected.
- Conan packages are not supported at the moment. Conan scan is available when uploaded to Artifactory and will be supported in the on-demand binary scan in later versions.