

CyberSecurityUP / Public CVEs (Joas Antonio)

Last active 2 years ago

☆ Star

<> Code Revisions 3 ☆ Stars 1

Public CVEs (Joas Antonio)

```
1 CVE -2018-18405:
2 O jQuery v2.2.2 permite o XSS por meio de um atributo onerror criado de um elemento IMG.
3 Reference: https://owasp.org/www-community/attacks/xss/ -
4 https://www.imperiva.com/learn/application-security/cross-site-scripting-xss-attacks/ -
5 https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/xss.md -
6
7
8 CVE-2019-19517:
9 Os dispositivos Intelbras RF1200 1.1.3 permitem que o CSRF faça a autenticação no
10 login.html sem a necessidade de acessar a interface de login, possibilitando força bruta e
11 até raspagem, conforme demonstrado pelo lançamento de um processo obsoleto.
12 Reference: https://www.youtube.com/watch?v=5ZQ9yIomSWA /
13 https://portswigger.net/web-security/csrf /
14 https://www.youtube.com/watch?v=13QPmRuhbHU
15
16 CVE-2019-19514: Os dispositivos
17 Ayision Ays-WR01 v28K.RPT.20161224 permitem o XSS armazenado nas configurações
18 básicas do repetidor por meio de um SSID.
19 Reference: https://www.youtube.com/watch?v=mKE0-Zij2lc -
20 https://www.rapid7.com/resources/ssid-xss-vulnerabilities-explained/
21
22 CVE-2019-19515: Os dispositivos
23 Ayision Ays-WR01 v28K.RPT.20161224 permitem XSS armazenado nas configurações
24 sem fio.
25 Reference: https://www.youtube.com/watch?v=mKE0-Zij2lc /
26 https://www.rapid7.com/resources/ssid-xss-vulnerabilities-explained/
27 Foi utilizado a mesma prova do conceito, só muda o campo de formulário aonde foi
28 injetado
29
30 CVE-2020-5517:
31 O CSRF no URI / login no BlueOnyx 5209R permite que um invasor acesse o painel e
32 execute raspagem ou outra análise.
33 Reference: https://portswigger.net/web-security/csrf /
34 https://www.youtube.com/watch?v=13QPmRuhbHU /
35 https://www.youtube.com/watch?v=I0W45zfnlWo /
36 https://www.youtube.com/watch?v=ArBndCZWwEs
37
38 CVE-2020-7983:
39 um problema de CSRF no login.asp nos dispositivos Ruckus R500 3.4.2.0.384 permite que
40 atacantes remotos acessem o painel de login
41 Reference: https://portswigger.net/web-security/csrf //
42 https://www.youtube.com/watch?v=45730XpG4u4&t=28s
43
44 CVE-2020-8033:
45 Os dispositivos Ruckus R500 3.4.2.0.384 permitem XSS através do campo index.asp
46 Device Name.
47 Reference: https://www.youtube.com/watch?v=myycj3nhLZ4
48
49 CVE-2020-8829: O
50 CSRF nos dispositivos Intelbras CIP 92200 permite que um invasor acesse o painel e
51 execute raspagem ou outra análise.
52 Reference: https://www.youtube.com/watch?v=8t10pzAZL1o /
53 https://portswigger.net/web-security/csrf
54
55 CVE-2020-8830: O CSRF no login.asp nos dispositivos Ruckus R500 permite que um invasor acesse o painel
56 e use scripts para executar raspagem ou outra análise através do campo SUBCA-1 na tela
57 Wireless Admin.
58 Reference: https://www.youtube.com/watch?v=zZxnOYhpmSA
```