CyberSecurityUP / **Public CVEs (Joas Antonio)**

Last active 2 years ago

Public CVEs (Joas Antonio)

```
CVE -2018-18405:
O jQuery v2.2.2 permite o XSS por meio de um atributo onerror criado de um elemento IMG.
Reference: https://owasp.org/www-community/attacks/xss/ -
https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/ -
https://github.com/EdOverflow/bugbounty-cheatsheet/blob/master/cheatsheets/xss.md -


CVE-2019-19517:
Os dispositivos Intelbras RF1200 1.1.3 permitem que o CSRF faça a autenticação no
login.html sem a necessidade de acessar a interface de login, possibilitando força bruta e
até raspagem, conforme demonstrado pelo lançamento de um processo obsoleto.
Reference: https://www.youtube.com/watch?v=5ZQ9yIomSWA /
https://portswigger.net/web-security/csrf /
https://www.youtube.com/watch?v=13QPmRuhbhU

CVE-2019-19514: Os dispositivos
Ayision Ays-WR01 v28K.RPT.20161224 permitem o XSS armazenado nas configurações
básicas do repetidor por meio de um SSID.
Reference: https://www.youtube.com/watch?v=mKE0-Zij2lc -
https://www.rapid7.com/resources/ssid-xss-vulnerabilities-explained/

CVE-2019-19515: Os dispositivos
Ayision Ays-WR01 v28K.RPT.20161224 permitem XSS armazenado nas configurações
sem fio.
Reference: https://www.youtube.com/watch?v=mKE0-Zij2lc /
https://www.rapid7.com/resources/ssid-xss-vulnerabilities-explained/
Foi utilizado a mesma prova do conceito, só muda o campo de formulário aonde foi
injetado

CVE-2020-5517:
O CSRF no URI / login no BlueOnyx 5209R permite que um invasor acesse o painel e
execute raspagem ou outra análise.
Reference: https://portswigger.net/web-security/csrf /
https://www.youtube.com/watch?v=13QPmRuhbhU /
https://www.youtube.com/watch?v=I0W45zfnlWo /
https://www.youtube.com/watch?v=ArBndCZWwEs

CVE-2020-7983:
um problema de CSRF no login.asp nos dispositivos Ruckus R500 3.4.2.0.384 permite que
atacantes remotos acessem o painel de login
Reference: https://portswigger.net/web-security/csrf //
https://www.youtube.com/watch?v=4573oXpG4u4&amp;t=28s

CVE-2020-8033:
Os dispositivos Ruckus R500 3.4.2.0.384 permitem XSS através do campo index.asp
Device Name.
Reference: https://www.youtube.com/watch?v=myycj3nhLZ4

CVE-2020-8829: O
CSRF nos dispositivos Intelbras CIP 92200 permite que um invasor acesse o painel e
execute raspagem ou outra análise.
Reference: https://www.youtube.com/watch?v=8tlOpzAZL1o /
https://portswigger.net/web-security/csrf

CVE-2020-8830:  O CSRF no login.asp nos dispositivos Ruckus R500 permite que um invasor acesse o painel
e use scripts para executar raspagem ou outra análise através do campo SUBCA-1 na tela
Wireless Admin.
Reference: https://www.youtube.com/watch?v=zZxnOYhpmSA
```