dharmeshbaskaran / **CVE-2020-19202**

Created last year

Authenicated Stored XSS in IPFire 2.21

CVE-2020-19202

```
CVE-2020-19202
========================================================================
* Authenicated Stored XSS in Captive.cgi
* Affected Product: IPFire 2.21 (x86_64) - Core Update 130
* Vendor: IPFire
* Vulnerability Class: Stored Cross-Site Scripting
* Status: Fixed
* Author: Dharmesh Baskaran
========================================================================

=== SUMMARY ===

An authenticated Stored XSS (Cross-site Scripting) exists in the "captive.cgi" Captive Portal via the "Title of Login Page" text box or "TI

=== TECHNICAL DESCRIPTION ===

An authenticated Stored XSS (Cross-site Scripting) exists in the (https://localhost:444/cgi-bin/captive.cgi) Captive Portal via the "Title

=== REMEDIATION ===

They removed       $settings{'TITLE'}                    = $cgiparams{'TITLE'};
They added         $settings{'TITLE'}                    = &Header::escape($cgiparams{'TITLE'});

=== DISCLOSURE TIMELINE ===

2019-05-07: Vulnerability disclosed via email to IPFire Team
2019-05-07: Acknowlegement from IPFire Team
2019-05-09: Fixed in IPFire 2.23 - Core Update 132: https://git.ipfire.org/?p=ipfire-2.x.git;a=commitdiff;h=462bc3d1595df12dd16a5d93f86a48e

========================================================================
```