⌥ master ⌄   ···

BugReport / CVE-2020-21733

⬤ **Gr3gPr1est** Create CVE-2020-21733   ⊙ History

⊞ **1 contributor**

---

46 lines (25 sloc) │ 998 Bytes   ···

```
 1   Vulnerability Type:
 2   Cross Site Scripting (XSS)
 3
 4
 5   ● Additional Information:
 6   https://github.com/Gr3gPr1est/BugReport/blob/master/SAGEM_F%
 7   40ST3686_v1.0_HUN_3.97.0_XSS_Vuln..pdf
 8
 9
10   ● Affected Component:
11   RgDiagnostics.asp, RgDdns.asp, RgFirewallEL.asp,
12   RgVpnL2tpPptp.asp
13
14
15   ● Attack Typeo: Remote
16
17
18   ● Impact Code execution: true
19
20
21   ● Attack Vectors:
22   The SagemCom router RgDiagnostics.asp, RgDdns.asp,
23   RgFirewallEL.asp, RgVpnL2tpPptp.asp vulnerable to XSS.
24
25
26   ● Reference:
27   http://sagemcom.com http://sagemcomfst3686v10hun3970.com
28   https://github.com/Gr3gPr1est/BugReport/blob/master/SAGEM_F%
29   40ST3686_v1.0_HUN_3.97.0_XSS_Vuln..pdf
30
31
32   ● Vendor of Product:
33   Sagemcom
34
35
36   ● Affected Product Code Base:
37   SAGEMCOM_F@ST3686_v1.0_HUN_3.97.0 v1.0 HUN 3.97.0
38
39
40   ● Suggested description:
41   Sagemcom F@ST3686 v1.0 HUN 3.97.0 v1.0 HUN 3.97.0 has XSS) via RgDiagnostics.asp, RgDdns.asp, RgFirewallEL.asp, RgVpnL2tpPptp.asp.
42
43
44   sub.zer0d4y@gmail.com
45
46   Use CVE-2020-21733 for this vulnerability.
```