New Mirai Variant Expands, Exploits CVE-2020-10173

blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173/

July 8, 2020

IoT

We discovered a new Mirai variant that exploits nine vulnerabilities, most notable of which is CVE-2020-10173 in Comtrend VR-3033 routers which we have not observed exploited by past Mirai variants.

By: Augusto Remillano II, Jemimah Molina July 08, 2020 Read time: (words)

Content added to Folio

We discovered a new Mirai variant (detected as IoT.Linux.MIRAI.VWISI) that exploits nine vulnerabilities, most notable of which is CVE-2020-10173 in Comtrend VR-3033 routers which we have not observed exploited by past Mirai variants.

This discovery is a new addition to the Mirai variants that appeared in the past few months, that include SORA, UNSTABLE, and Mukashi. The case, however, showcases the ever-expanding arsenal of vulnerabilities new Mirai variants are equipped with by their developers.

The vulnerabilities

The vulnerabilities used by this Mirai variant consist of a combination of old and new that help cast a wide net encompassing different types of connected devices. The nine vulnerabilities used in this campaign affect specific versions of IP cameras, smart TVs, and routers, among others.

As mentioned earlier, the most notable of these vulnerabilities is CVE-2020-10173, a Multiple Authenticated Command injection vulnerability found in Comtrend VR-3033 routers. Remote malicious attackers can use this vulnerability to compromise the network managed by the router.

Only a proof of concept (POC) has been released for this vulnerability, with no reported exploit at large before this Mirai variant. Figure 1 serves as evidence of how this vulnerability is used by the sample.

Code snippet showing the use of CVE-2020-10173

Figure 1. Code snippet that shows the use of CVE-2020-10173

Another relatively recent vulnerability also used in this campaign is Netlink GPON Router 1.0.11 RCE. Discovered this year, it was reportedly exploited by the Bashlite/Gafgyt variant Hoaxcalls.

Code snippet showing the use of Netlink GPON Router 1.0.11 RCE

Figure 2. Code snippet that shows the use of Netlink GPON Router 1.0.11 RCE

Aside from the two, the variant makes use of mostly old vulnerabilities which have been used in past campaigns. The two code snippets shown in figures 3 and 4 serve as examples of old vulnerabilities written in the variant’s code.

Code snippet showing the use of LG SuperSign EZ CMS 2.5 - Remote Code Execution

Figure 3. Code snippet that shows the use of LG SuperSign EZ CMS 2.5 - Remote Code Execution

Code snippet showing the use of Linksys E-series - Remote Code Execution

Figure 4. Code snippet that shows the use of Linksys E-series - Remote Code Execution

In addition to these examples, the remaining five old vulnerabilities that were exploited by the variant are the following:

- AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities
- D-Link Devices - UPnP SOAP Command Execution
- MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution
- Symantec Web Gateway 5.0.2.8 Remote Code Execution
- ThinkPHP 5.0.23/5.1.31 - Remote Code Execution

Brute-force capabilities

A hallmark of Mirai variants is the use of Telnet and Secure Shell (SSH) brute-forcing as evidenced by our sample. This variant also used the typical XOR encryption (with the XOR key: 0x04) to hide the credentials that it uses to attack vulnerable devices. The credentials we extracted are listed here.

Extracted credentials		
0	GM8182	ROOT500
1001chin	grouter	solokey
1111	guest	svgodie
1234	h3c	swsbzkgn
12345	hg2x0	system
123456	hi3518	t0talc0ntr0l4!
20080826	huigu309	taZz@23495859
54321	hunt5759	telecomadmin
5up	iDirect	telnet
666666	ipcam_rt5350	telnetadmin
88888888	iwkb	tl789
abc123	juantech	tsgoingon
admin	jvbzd	twe8ehome
ahetzip8	klv123	user
anko	nflection	vizxv
antslq	nmgx_wapia	win1dows
ascend	oelinux123	xc3511
blender	pass	xmhdipc
cat1029	password	zhongxing
changeme	private	zlxx.
default	realtek	zsun1188
dreambox	root	Zte521

Conclusion and security recommendations

The use of CVE-2020-10173 in this variant’s code shows how botnet developers continue to expand their arsenal to infect as many targets as possible and take advantage of the opening afforded by unpatched devices. Newly discovered vulnerabilities, in particular, offer better chances for cybercriminals. Users, not knowing that a vulnerability even exists, might be unable to patch the device before it is too late.

In the future, it would be wise to expect this vulnerability might be used in new DDoS botnets like Mirai. As monitoring of such botnets show, handlers tend to copy each other’s techniques, including lists of vulnerabilities and credentials that increase their chance of success.

For devices to remain safe from the usual tactics of botnet malware, users need to follow best practices in securing their connected devices. These include the following:

- Patch vulnerabilities and apply updates as soon as they become available.
- Use network segmentation to limit the spread of potential infections.
- Use strong passwords and quickly change default ones.
- Apply secure configurations for devices to limit unforeseen openings for infection.

Connected devices can also be protected by security software such as the Trend Micro™ Home Network Security and Trend Micro™ Home Network Security SDK solutions, which can check internet traffic between the router and all connected devices as well as help users asses for vulnerabilities.

Trend Micro™ Deep Discovery™ Inspector also protects customers from this attack via these DDI rules:

- 2452 - Wget Commandline Injection
- 2544 - JAWS Remote Code Execution Exploit - HTTP (Request)
- 2575 - Command Injection via UPnP SOAP Interface - HTTP (Request)
- 2692 - LINKSYS Unauthenticated Remote Code Execution Exploit - HTTP (Request)
- 2713 - AVTECH Command Injection Exploit - HTTP (Request)
- 2786 - ThinkPHP 5x Remote Code Execution - HTTP (Request)
- 2865 - CVE-2018-17173 LG Supersign Remote Code Execution - HTTP (Request)
- 4689 - Comtrend - Remote Command Execution Exploit - HTTP (REQUEST)

Indicators of compromise (IoCs)

SHA256	Old Detection	New Detection
66545fffeed4f413827f9dc51d2444aaa772adf4d44f65662356b1301e45390d	Backdoor.Linux.MIRAI.VWIUJ	IoT.Linux.MIRAI.VWISI

Command and control (C&C) servers

- methcnc[.]duckdns[.]org
- methscan[.]duckdns[.]org