



Jeff Welton

Sales Manager, Central USA
Nautel



Matt Herdon

Product Manager and Marketing
Nautel



Shane Toven

Senior Broadcast Engineer
K-LOVE & Air1 Media Networks



Episode #76

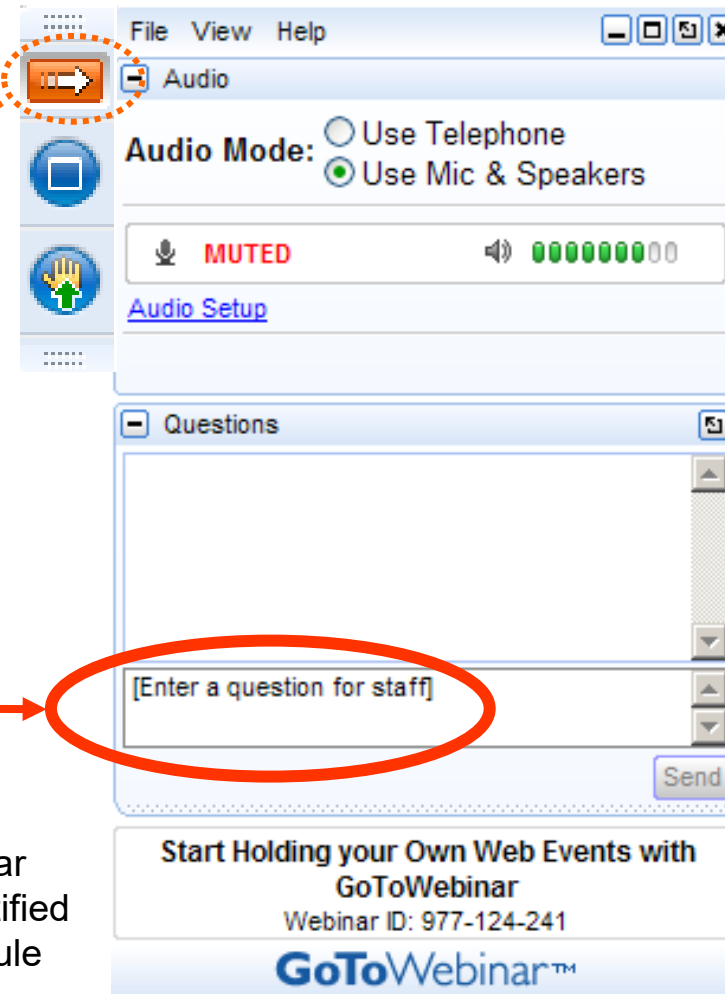
IT Security Questions

**(to Ask Your
Manufacturer)**

Your questions please?

(if you don't see the control panel, click on the orange arrow icon to expand it)

Please enter your questions in the text box of the webinar control panel (remember to press send)



The screenshot shows a GoToWebinar control panel window. At the top, there is a menu bar with 'File', 'View', and 'Help'. Below the menu bar, there is a section for 'Audio' settings. An orange arrow icon is circled in red and has a dotted orange line pointing to it. The audio settings include 'Audio Mode' with two radio buttons: 'Use Telephone' (unselected) and 'Use Mic & Speakers' (selected). Below this, there is a 'MUTED' indicator with a microphone icon and a volume level indicator showing 00. A link for 'Audio Setup' is visible. Below the audio settings, there is a 'Questions' section. A text box with the placeholder text '[Enter a question for staff]' is circled in red, and a solid red arrow points to it from the left. A 'Send' button is located to the right of the text box. At the bottom of the control panel, there is a promotional banner for 'Start Holding your Own Web Events with GoToWebinar' with the Webinar ID: 977-124-241 and the GoToWebinar logo.



Remember: The completion of a Nautel webinar qualifies for $\frac{1}{2}$ SBE re-certification credit, identified under Category I of the Re-certification Schedule for SBE Certifications.

Advance Questions

What is your mother's maiden name and what street did you grow up on? Asking for a friend.



FCC Acts to Strengthen the Security of Nation's Alerting Systems

Full Title: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, et al., PS Docket No. 15-94 et al., Notice of Proposed Rulemaking

Document Type(s): Notice of Proposed Rulemaking

Bureau(s): Public Safety and Homeland Security

Description:

FCC launches a rulemaking to improve the security and reliability of the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA)

DA/FCC #: FCC-22-82

Docket/RM: 15-94, 15-91, 22-329

Document Dates

Released On: Oct 27, 2022

Adopted On: Oct 27, 2022

Issued On: Oct 27, 2022

Tags:

Cybersecurity - Disaster Response -
Emergency Alert System - Emergency
Communications - Network Reliability -
Wireless Emergency Alerts

<https://www.fcc.gov/document/fcc-acts-strengthen-security-nations-alerting-systems>



TOTAL RESULTS

11

TOP COUNTRIES



United States	8
Brazil	1
Canada	1
Switzerland	1

TOTAL RESULTS

727

TOP COUNTRIES



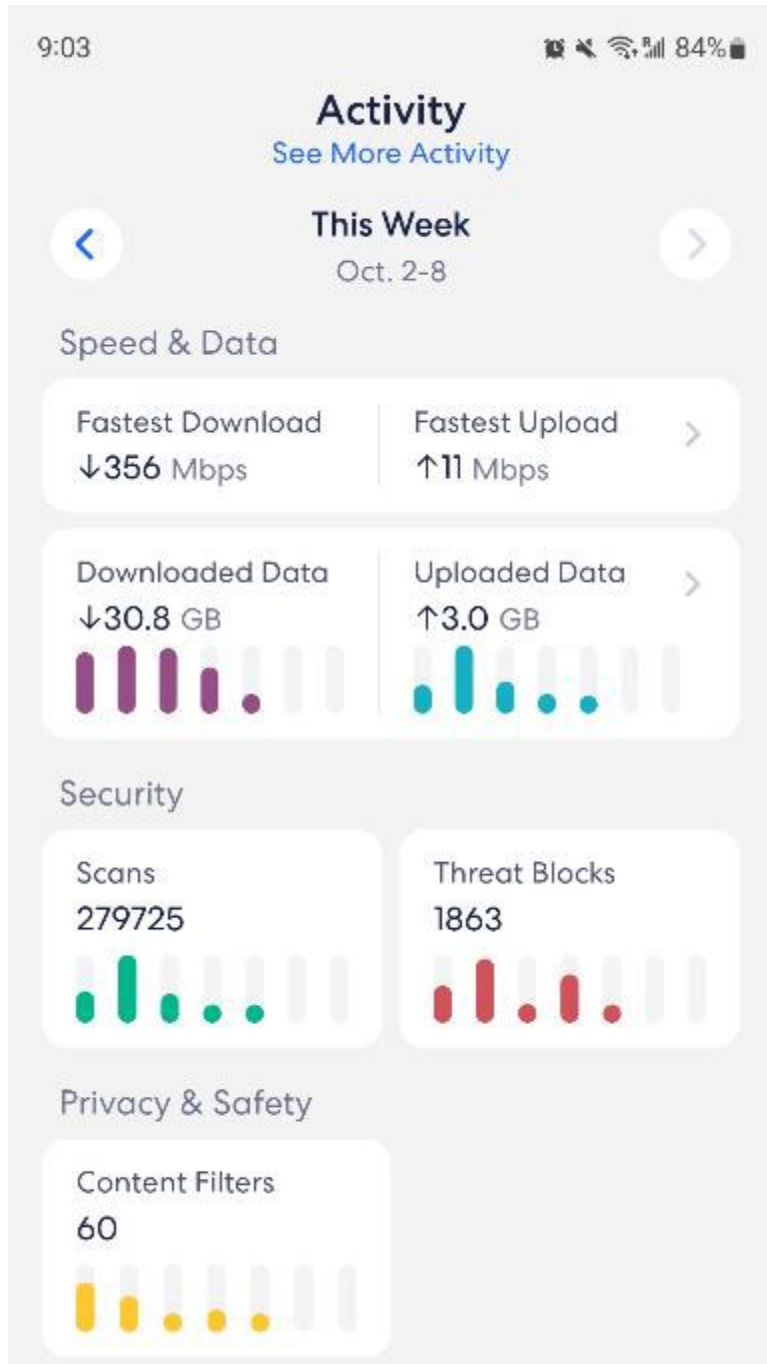
United States	694
Canada	31
Germany	1
Puerto Rico	1

Top 5 Computer Security Vulnerabilities

- 1) **Hidden Backdoor Programs**
- 2) **Superuser or Admin Account Privileges**
- 3) **Automated Running of Scripts without Malware/Virus Checks**
- 4) **Unknown Security Bugs in Software or Programming Interfaces**
- 5) **Unencrypted Data on the Network**

<https://www.compuquip.com/blog/computer-security-vulnerabilities>

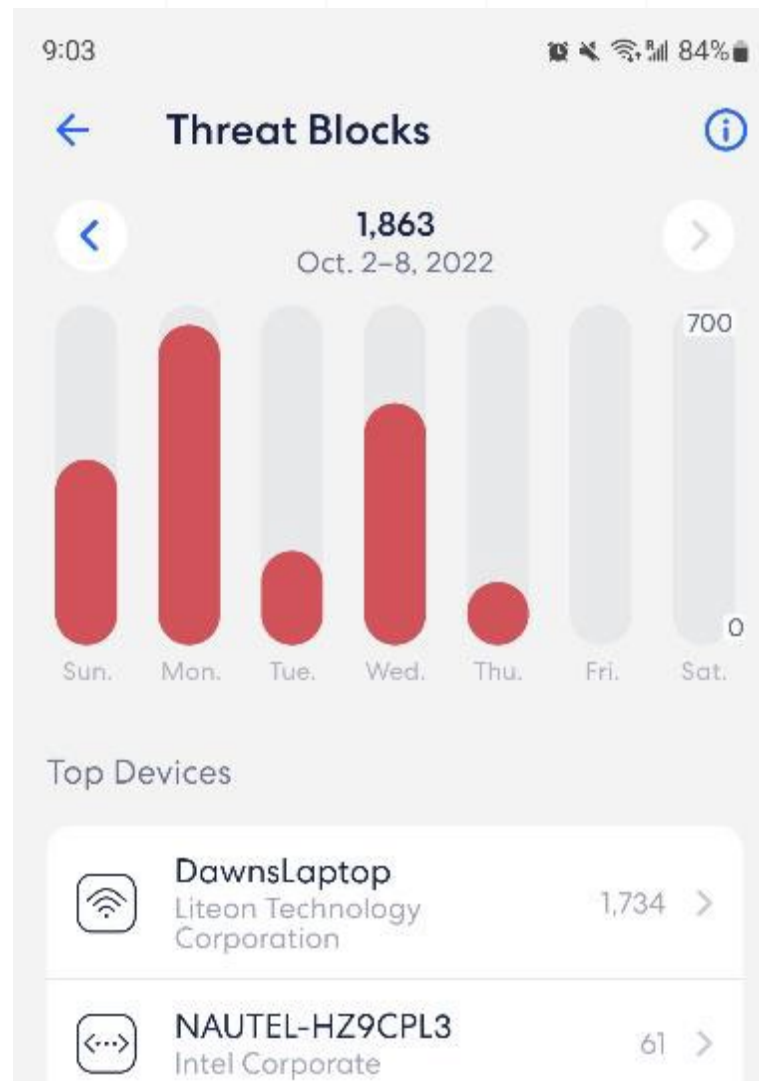




Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing ↗

“Jeff’s home IP address”



Note: No results found



“As for things manufacturers could do...I think we're (mostly) on the same page there too. Let's face it. Broadcast manufacturers (as a general rule) are HORRIBLE about infosec. This is a mix of making it "easier" for end users, and for the manufacturers to support-both of which are pretty poor excuses. I propose the following minimums...

1: Enforce strong passwords.

2: Provide (and enable by default) a basic NAT and/or port filtering firewall... If not a cloud or proxy type service, perhaps some sort of dedicated client with VPN tunneling built in, with a VPN server built into the equipment.

3: Critical updates pushed to equipment by default with automatic installation by default, but with the user's ability to select a maintenance window when they are installed... As it stands, most broadcast equipment manufacturers are terrible about making these updates available in a timely manner, if at all.

There is a LOT of room for improvement. Now it's a matter of both sides taking their share of responsibility to keep this critical infrastructure secure.”



Open Ports

80

443

4443

8009

8081

10443

51235

55553

Open Ports

80

1194

1723

4545

5900

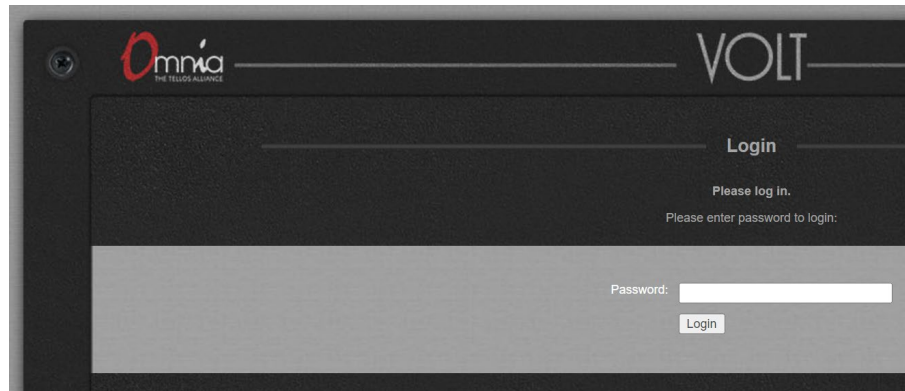
8080

8088

9000

9001

9002



Challenges include many who:

- Vehemently do not want updates happening outside of their total control and timing
- Don't want to disturb a working stable transmitter
- Don't like the hassle of managing passwords
- Have never been impacted by a hack so requiring protection they will benefit from can at least be a hard sell
- Have IT departments for which policies range from lax to extremely rigid
-
- **Primary Issues**
-
- Unmaintained Linux OS (no security patches)
- Default/weak passwords
- No password enforcement
- Hackable transmitter
- Hackable remote control
- Internet connectivity
 - Enables hacking
 - If severely limited, updates are necessarily in person at site via USB
- Usability – the more we do the worse it gets, despite it protecting against really bad things

I try to keep track of all the vulnerabilities, but it's getting harder and harder as time passes. RedHat alone sends out as many as a dozen reports a day; most are for minor bug fixes, but a few are true show-stoppers. As I write this, I just installed a newly-patched Linux kernel on our web server. All of those RedHat advisories made me suspect that it was time to upgrade. Indeed it was.

Stephen Poole, from Crawford Media Group's January engineering newsletter



Pi-hole - pihole

Not secure | 192.168.88.100/admin/index.php

Apps Facebook - Log in o... Notebook for Progr... codplayer 1.1: Pyth... CD AUDIO pygame Solarflare SFN7501... KYDronePilot/hdfm... XTRX | Crowd Supply StcloudState.edu E... Reading list

Pi-hole hostname: pihole

Status
 ● Active
 ● Load: 0.00
 ● Memory usage: 22.7%

MAIN NAVIGATION

- Dashboard
- Query Log
- Long-term data
- Whitelist
- Blacklist
- Group Management
- Disable
- Tools
- Settings
- Local DNS
- Logout
- Donate
- Documentation

Total queries (54 clients)
85,357

Queries Blocked
8,047

Percentage Blocked
9.4%

Domains on Blocklist
100,077

Total queries over last 24 hours

Client activity over last 24 hours

Query Types

- A (IPv4)
- AAAA (IPv6)
- SRV
- PTR
- TXT
- OTHER
- HTTPS

Upstream servers

- blocklist
- cache
- dns.google#53
- dns.google#53



Online Information



Webinars

<https://www.nautel.com/resources/webinars/>



Nautel Waves Newsletter

<https://www.nautel.com/newsletters/>



YouTube

<http://www.youtube.com/user/NautelLtd>



Online Info, such as the Broadcasters' Desktop Resource

<https://www.thebdr.net/>

THANK YOU!

