CYBERSECURITY ASSESSMENT AT JTNM – TEST @RIEDEL AUG'19 RESULTS & RECOMMENDATIONS

Gerben Dierick (VRT)
Alvaro Marin (RTVE)
Adi Kouadio (EBU)

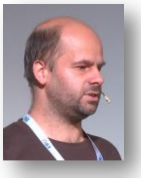
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

1. BACKGROUND
2. TEAM
3. TEST SET UP
4. FINDINGS RESULTS
5. CONCLUSIONS
6. ANNEX – VULNERABILITIES & MITIGATION PLANS DETAILED

WHY A CYBERSECURITY ASSESSMENT @ JTNM INTEROP?

- Several vendors in one location. Very practical to test lots of devices at once, and speak directly to technical people from the vendors.
- Connected Media Devices increase the attack surface at broadcaster premises. Need to prevent vulnerabilities to reduce risk.
- Broadcast industry still often ignores security. Need to raise industry maturity level.
- Media equipment vendors should embrace experience from IT development. We should not repeat mistakes but adopt best practices.

TEAM – MEMBERS OF EBU MCS GROUP



Mr Gerben Dierick is information security officer and network and security architect at Belgian public broadcaster VRT. He also lectures about information security at University College Leuven Limburg.

E-mail: gerben.dierick@vrt.be

Mr Alvaro Martin Santos is Cybersecurity Technical Officer in RTVE the Spanish national broadcaster, where he worked on IT Security and IAM. He is a Computer Science Engineer and is pursuing a PhD in Industrial Engineering, with a specialization in Security of IP broadcasting technologies at UNED - Universidad Nacional de Educación a Distancia (Spain).

E-mail: alvaro.martin@rtve.es

Mr Adi Kouadio is Senior Program Manager at EBU, where he coordinated the strategic group on Media Cybersecurity. He is a Communication Systems Engineer from EPFL (swiss federal institute of technology) and an Executive MBA from IMD business school (switzerland)

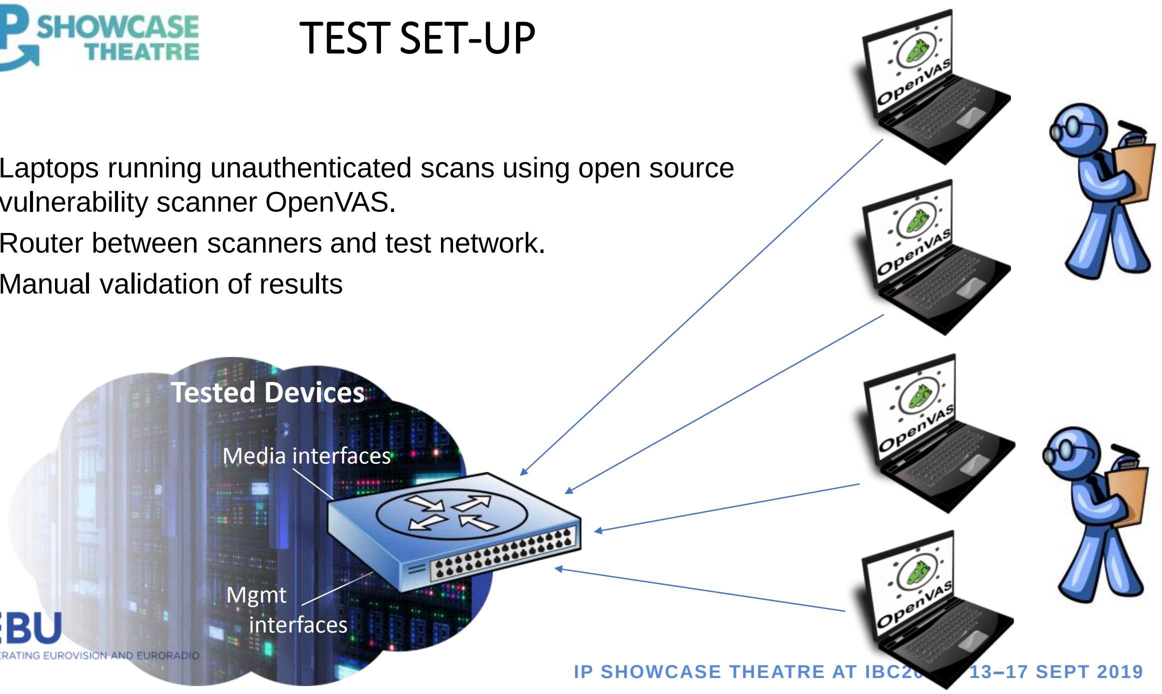
E-mail: kouadio@ebu.ch

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

IP SHOWCASE THEATRE

TEST SET-UP

- Laptops running unauthenticated scans using open source vulnerability scanner OpenVAS.
- Router between scanners and test network.
- Manual validation of results



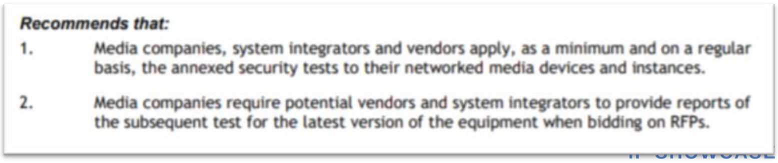
EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC20 13–17 SEPT 2019

IP SHOWCASE THEATRE

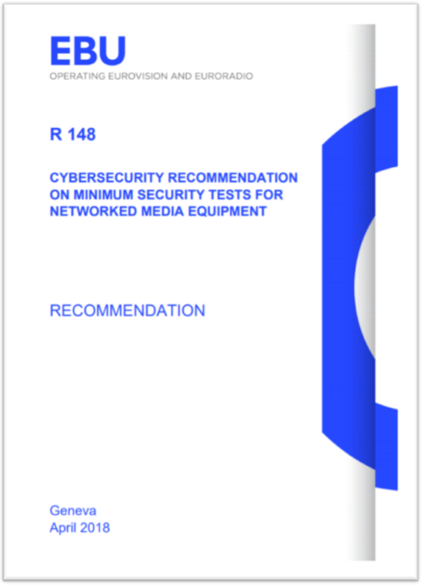
WHAT WAS TESTED…

- EBU Media CyberSecurity Group performed cybersecurity assessment of devices present at JTNM Tested event 08/2019 in Wuppertal, Germany
- Performed security scans are a subset of the tests recommended in EBU R148.
- **Disclaimer** : A security scan can prove the presence of security issues but it cannot prove the absence such issues.



Recommends that:

1. Media companies, system integrators and vendors apply, as a minimum and on a regular basis, the annexed security tests to their networked media devices and instances.
2. Media companies require potential vendors and system integrators to provide reports of the subsequent test for the latest version of the equipment when bidding on RFPs.



EBU
OPERATING EUROVISION AND EURORADIO

R 148

CYBERSECURITY RECOMMENDATION ON MINIMUM SECURITY TESTS FOR NETWORKED MEDIA EQUIPMENT

RECOMMENDATION

Geneva
April 2018

THEATRE AT IBC2019 : 13–17 SEPT 2019

THE SECURITY TEST IN NUMBERS…

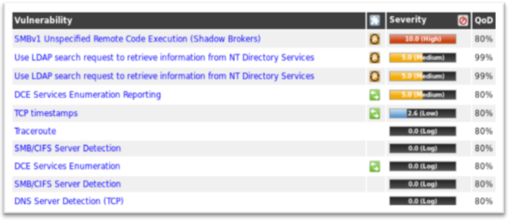
- All **65 535 TCP Ports** scanned, plus **100 Most used UDP** ports.
- **5** days testing **15 subnets**. Longest subnet scan took **26 hours**.
- **4** Laptops with OpenVAS running in parallel.
- **34** Vendors.
- **93 Devices** (70 Under Test) available for ST-2110 interop test.
- **68 Devices** Scanned (only the devices under test are considered in this report.)

EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

INTERPRETING VULNERABILITY SCANNER RESULTS

- The OpenVAS Scan results in a list of detected vulnerabilities with a severity level between 0,0 and 10
- **Always verify scanner findings and re-evaluate risk scores!**
- **Eliminate false positives** by manually checking reported vulnerabilities
- **EBU Custom ranking (severity from 1 to 4)** based on Cybersecurity Experts' Risk Assessment.



Vulnerability		Severity	QoD
SMBv1 Unspecified Remote Code Execution (Shadow Brokers)		10.0 (High)	80%
Use LDAP search request to retrieve information from NT Directory Services		5.0 (Medium)	99%
Use LDAP search request to retrieve information from NT Directory Services		5.0 (Medium)	99%
DCE Services Enumeration Reporting		5.0 (Medium)	80%
TCP timestamps		2.6 (Low)	80%
Traceroute		0.0 (Log)	80%
SMB/CIFS Server Detection		0.0 (Log)	80%
DCE Services Enumeration		0.0 (Log)	80%
SMB/CIFS Server Detection		0.0 (Log)	80%
DNS Server Detection (TCP)		0.0 (Log)	80%

EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

WHY CUSTOM RISK SCORES?

- We don't always agree with OpenVAS' severity levels.

  Example: Maximum severity score for presence of Discard Service (tcp/9), but no actual exploit known.

- **Context** can increase or decrease risk.

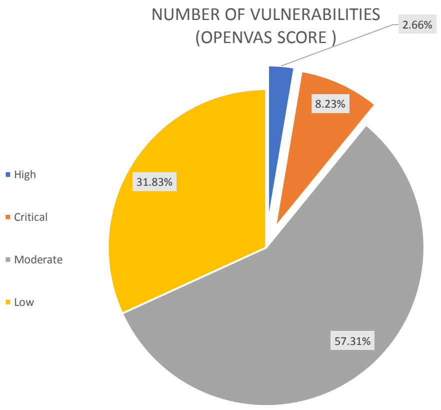
  Example: System meant to be accessible from the internet.

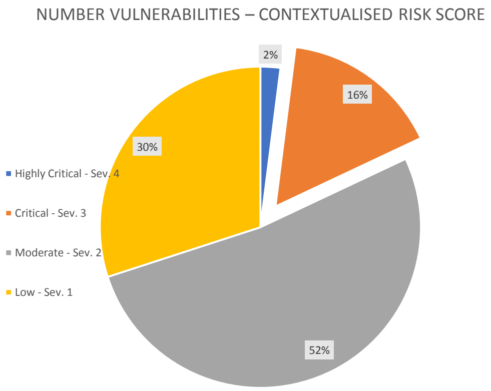
- **Combination** of less severe vulnerabilities can result in higher severity issue

  Example: **arbitrary file reading** combined with **hardcoded easy system password** results in fully **compromised system**.

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

CUSTOM RISK SCORE : WITH CONTEXTUALISED RISK 8% MORE CRITICAL VULNERABILITIES





IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

FINDINGS / RESULTS

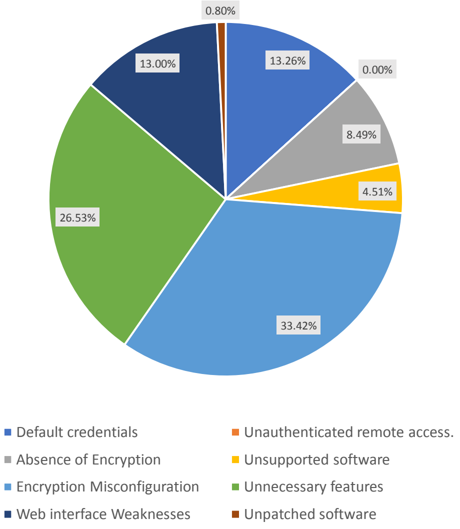
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

387 VULNERABILITIES FOUND : 5 MAIN VULNERABILITY CATEGORIES

- **Encryption Misconfiguration (33.4%)**
- **Unnecessary features (26.5%)**
- **Default credentials (13,2%)**
- **Web interface Weaknesses (13%)**
- **Absence of Encryption (8.5%)**

- Unsupported/Unpatched software (4.5%)

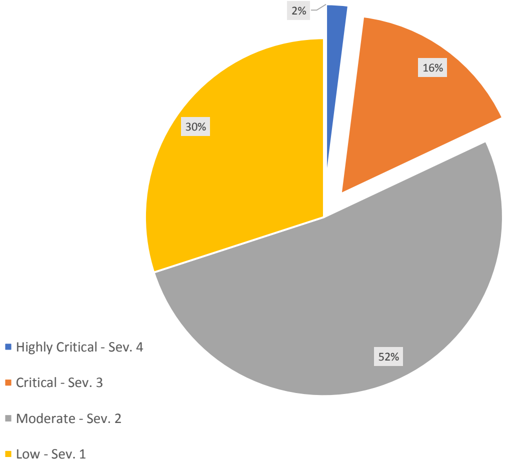
- Unauthenticated remote access (<1%)



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

387 VULNERABILITIES FOUND : 18% HIGHLY CRITICAL TO CRITICAL

- **18%** of vulnerabilities are critical to highly critical. EBU MCS will follow up to fix the issues.
- Most of the other moderate vulnerabilities are still potentially harmful but also easily fixed.



IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

387 VULNERABILITIES FOUND : 18% HIGHLY CRITICAL TO CRITICAL

High Severity Vunerability Types
Anonymous FTP Login (1)
Web interface without authentication (2)
OS End of Life
HTTP Directory Traversal
Default credentials (2)
Hardcoded (support) credentials
Mongoose < 6.15 Buffer Overflow Vulnerability

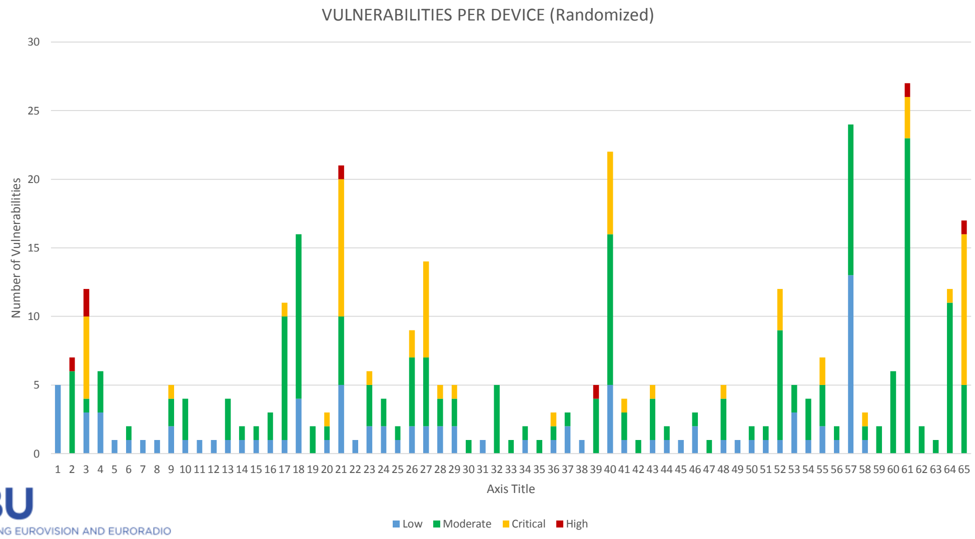
(1) Not always critical issue, depends on file system and user restrictions

(2) Can (generally) be fixed by configuration

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

IP SHOWCASE THEATRE

DISTRIBUTION OF VULNERABILITIES PER AFFECTED DEVICES

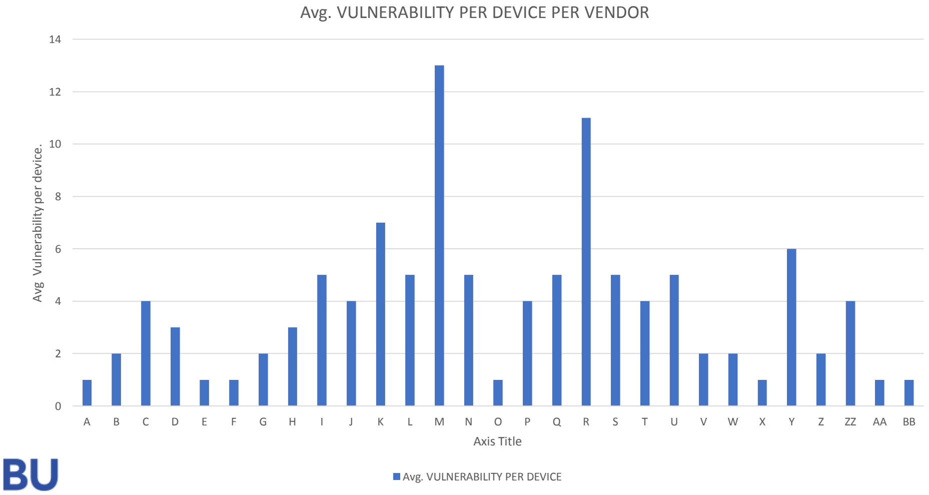


EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

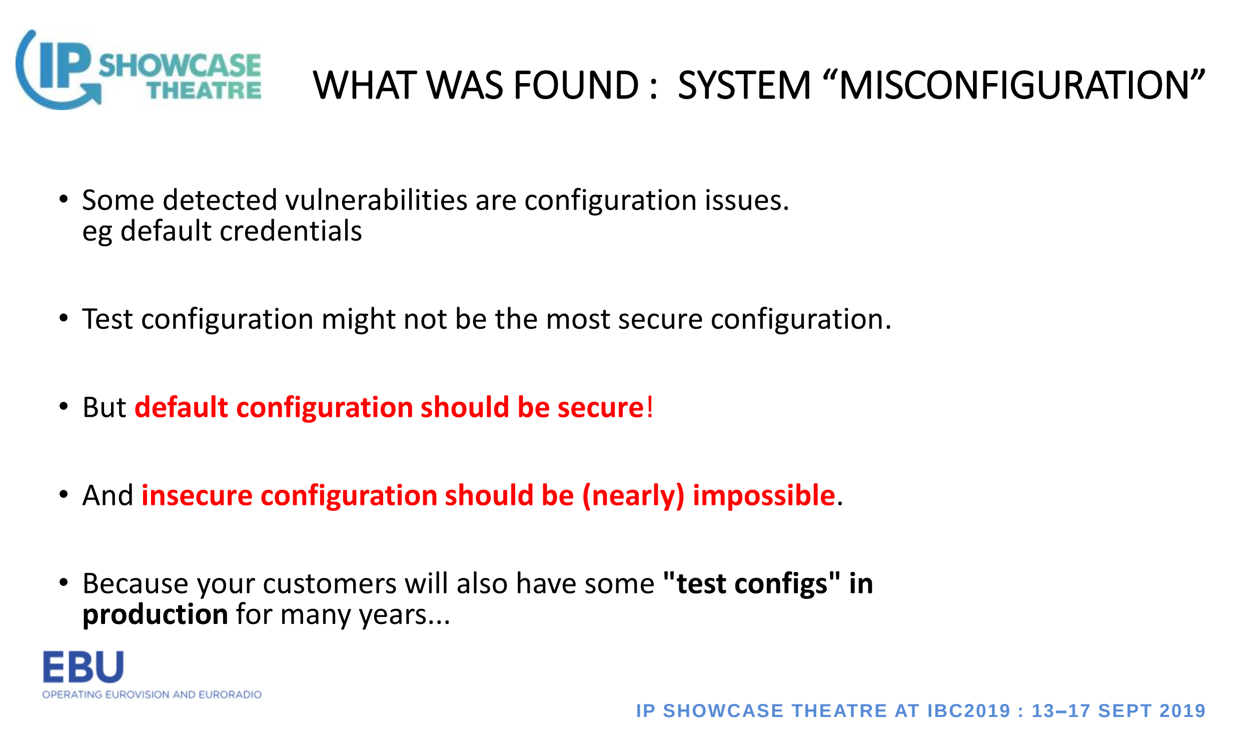
IP SHOWCASE THEATRE

AVERAGE NUMBER OF VULNERABILITIES PER AFFECTED DEVICES/VENDOR



EBU
OPERATING EUROVISION AND EURORADIO

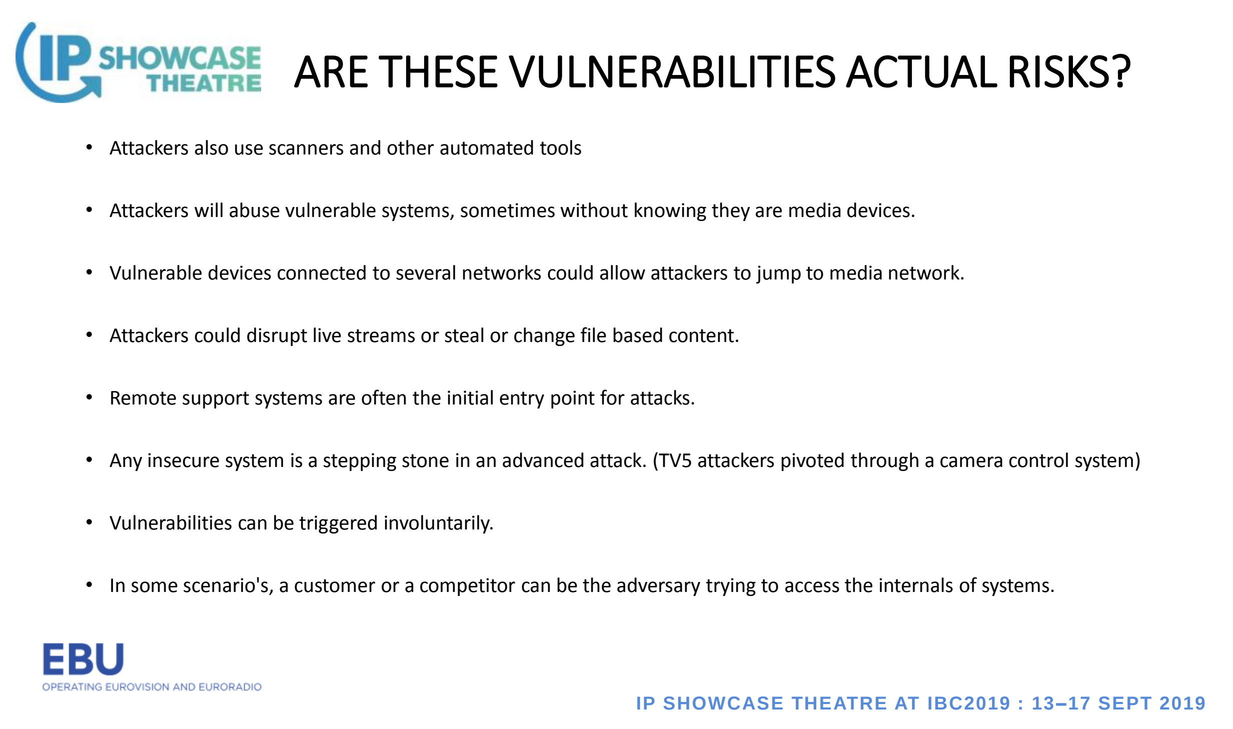
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



WHAT WAS FOUND : SYSTEM “MISCONFIGURATION”

- Some detected vulnerabilities are configuration issues.
  eg default credentials
- Test configuration might not be the most secure configuration.
- But **default configuration should be secure**!
- And **insecure configuration should be (nearly) impossible**.
- Because your customers will also have some **"test configs" in production** for many years...

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

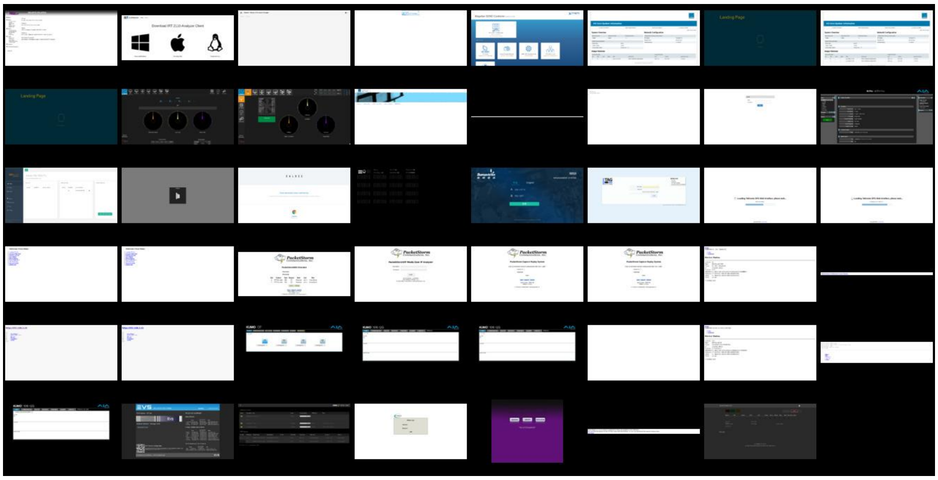


ARE THESE VULNERABILITIES ACTUAL RISKS?

- Attackers also use scanners and other automated tools
- Attackers will abuse vulnerable systems, sometimes without knowing they are media devices.
- Vulnerable devices connected to several networks could allow attackers to jump to media network.
- Attackers could disrupt live streams or steal or change file based content.
- Remote support systems are often the initial entry point for attacks.
- Any insecure system is a stepping stone in an advanced attack. (TV5 attackers pivoted through a camera control system)
- Vulnerabilities can be triggered involuntarily.
- In some scenario's, a customer or a competitor can be the adversary trying to access the internals of systems.

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

EXAMPLE TOOL: EYEWITNESS



Eyewitness scan of part of test network: All webinterfaces found on port 80

TALKING SECURITY WITH BROADCAST VENDORS

"Why would anybody attack this type of device?"

"Security is inconvenient, so we disabled it."

"This device should be in a closed network."

"This device should not be connected to the internet."

- Security = Don't trust anyone (not even the customer!)
- Unfortunately, security does not yet appear to be an important design requirements.
- Event participants were a bit hesitant at first, but very interested in our feedback.
- Good we're talking about security. We should keep the conversation going!

IP SHOWCASE THEATRE

CONCLUSIONS/ RECOMMENDATIONS

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

IP SHOWCASE THEATRE

RECOMMENDATIONS / NEXT STEPS

- The EBU MCS group will help the Vendors that had the most severe vulnerabilities to fix them (following EBU R160)
- Vendors are cordially invited to the EBU Media Cybersecurity Seminar (Geneva 22nd / 23rd October, see https://tech.ebu.ch/events/mcs2019)
- Vendors are encouraged to adopt a **responsible vulnerability disclosure program** highlighting the correct way to report security issues
  Come to the Presentation on the EBU booth (10F.20) Monday 16th September @ 16:00.
- Security should be part of the industry minimum requirement / minimum quality standard.
- Both vendors and users should perform security scans
  Contact EBU MCS for guidance (Mr Adi Kouadio - kouadio@ebu.ch)

EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

CONCLUSIONS

- There is lots of room for improvement, but luckily, we (as an industry) are improving !
- Very basic vulnerabilities found. No advanced skills needed to attack.
- Security scans are very useful, but expertise is needed to interpret the results
- Broadcast vendors are open to collaborate on issues.
- Broadcast vendors should learn from the IT industry best practices.

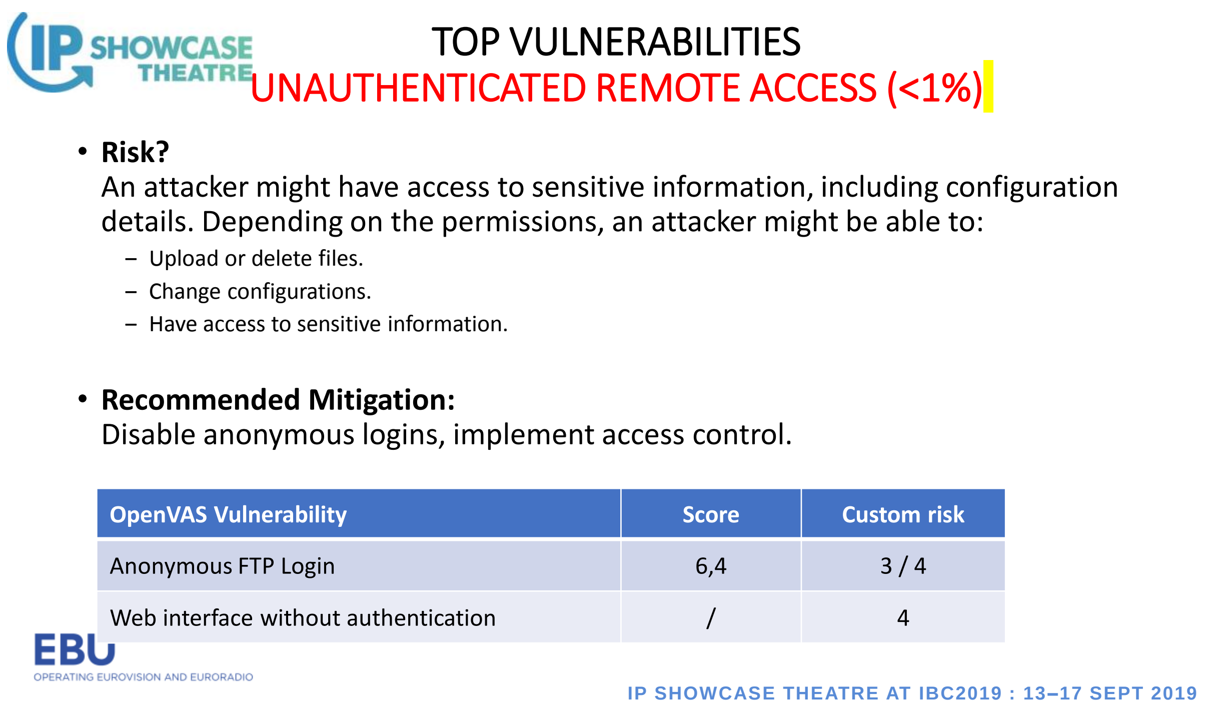
EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

ANNEX

- VULNERABILITIES AND MITIGATION PLAN DETAILED

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



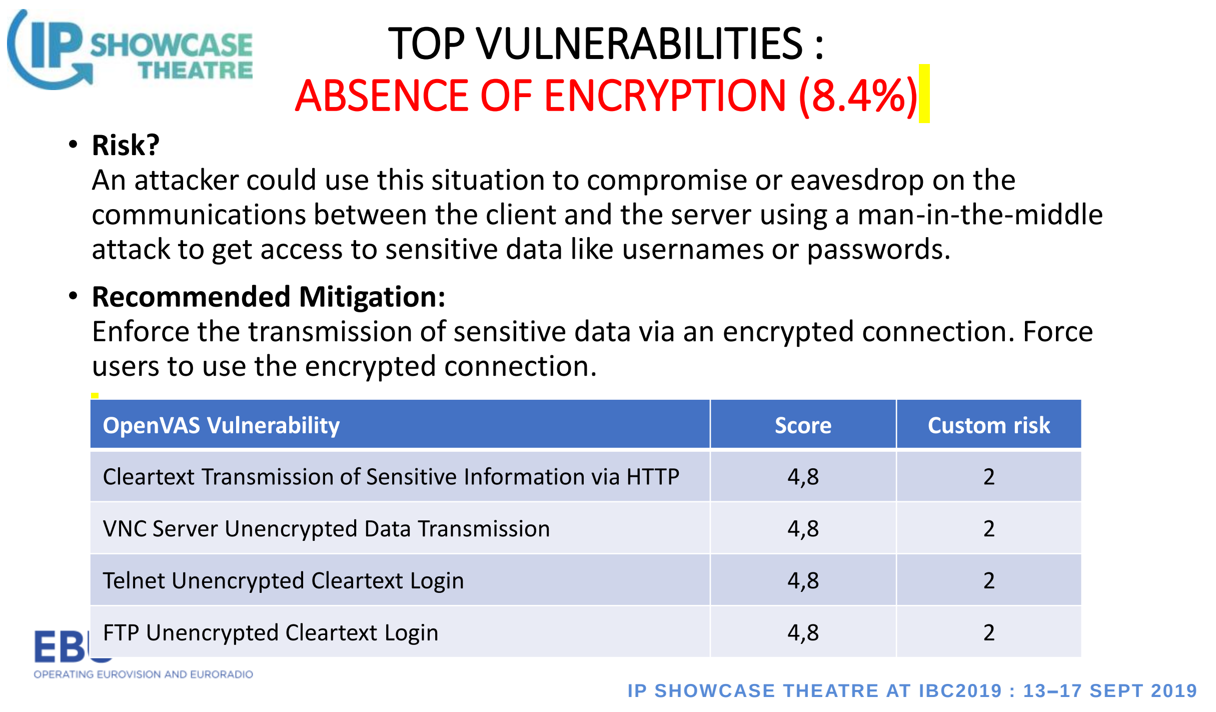
TOP VULNERABILITIES
UNAUTHENTICATED REMOTE ACCESS (<1%)

- **Risk?**
  An attacker might have access to sensitive information, including configuration details. Depending on the permissions, an attacker might be able to:
  - Upload or delete files.
  - Change configurations.
  - Have access to sensitive information.

- **Recommended Mitigation:**
  Disable anonymous logins, implement access control.

OpenVAS Vulnerability	Score	Custom risk
Anonymous FTP Login	6,4	3 / 4
Web interface without authentication	/	4

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

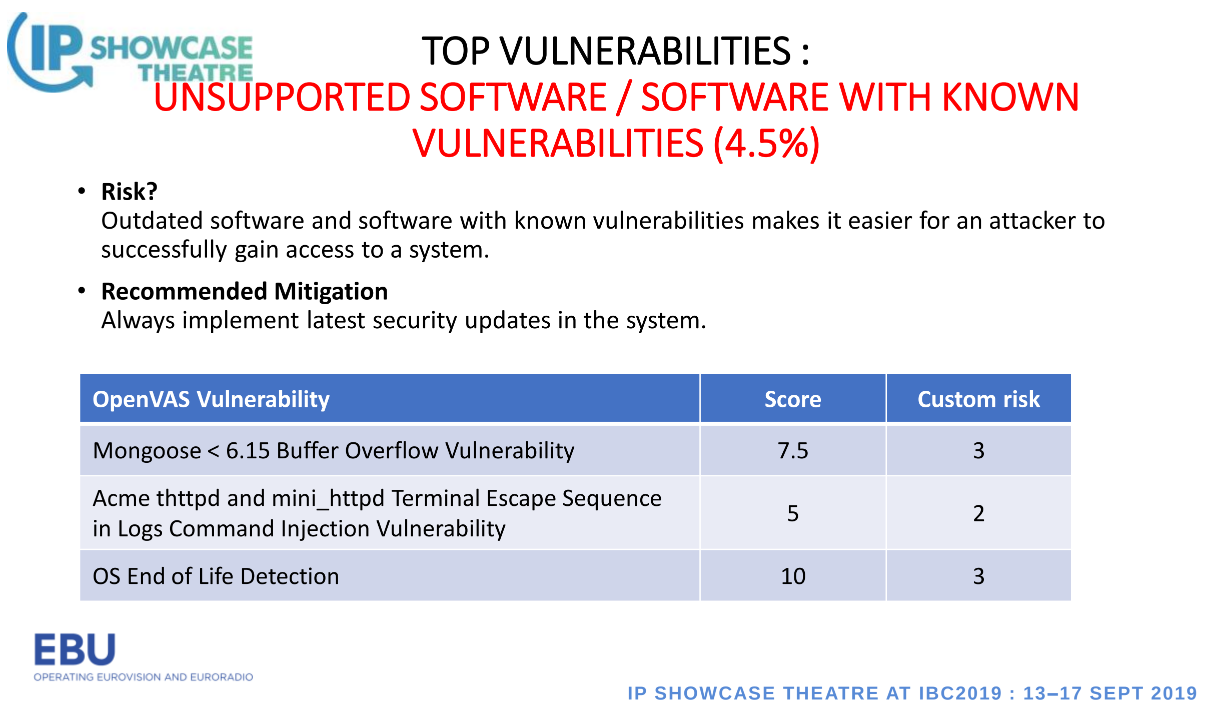


TOP VULNERABILITIES :
ABSENCE OF ENCRYPTION (8.4%)

- **Risk?**
  An attacker could use this situation to compromise or eavesdrop on the communications between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
- **Recommended Mitigation:**
  Enforce the transmission of sensitive data via an encrypted connection. Force users to use the encrypted connection.

OpenVAS Vulnerability	Score	Custom risk
Cleartext Transmission of Sensitive Information via HTTP	4,8	2
VNC Server Unencrypted Data Transmission	4,8	2
Telnet Unencrypted Cleartext Login	4,8	2
FTP Unencrypted Cleartext Login	4,8	2

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

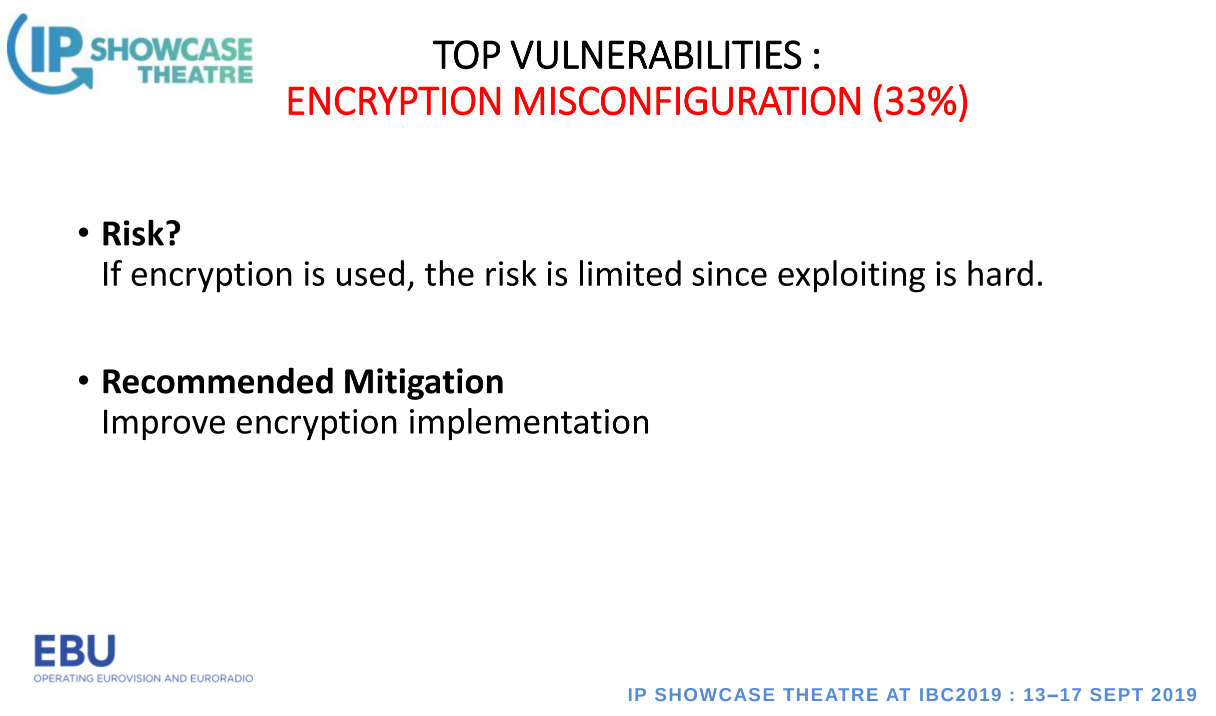


TOP VULNERABILITIES : UNSUPPORTED SOFTWARE / SOFTWARE WITH KNOWN VULNERABILITIES (4.5%)

- **Risk?**
  Outdated software and software with known vulnerabilities makes it easier for an attacker to successfully gain access to a system.
- **Recommended Mitigation**
  Always implement latest security updates in the system.

OpenVAS Vulnerability	Score	Custom risk
Mongoose < 6.15 Buffer Overflow Vulnerability	7.5	3
Acme thttpd and mini_httpd Terminal Escape Sequence in Logs Command Injection Vulnerability	5	2
OS End of Life Detection	10	3

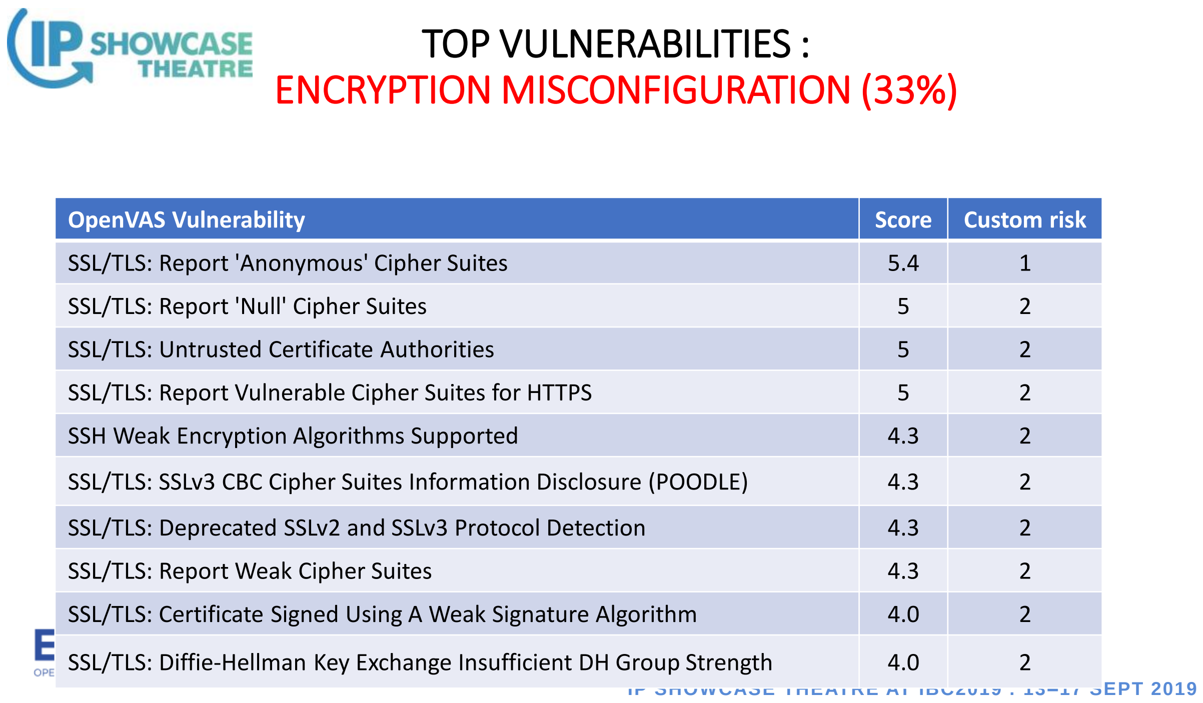
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



TOP VULNERABILITIES : ENCRYPTION MISCONFIGURATION (33%)

- **Risk?**
  If encryption is used, the risk is limited since exploiting is hard.
- **Recommended Mitigation**
  Improve encryption implementation

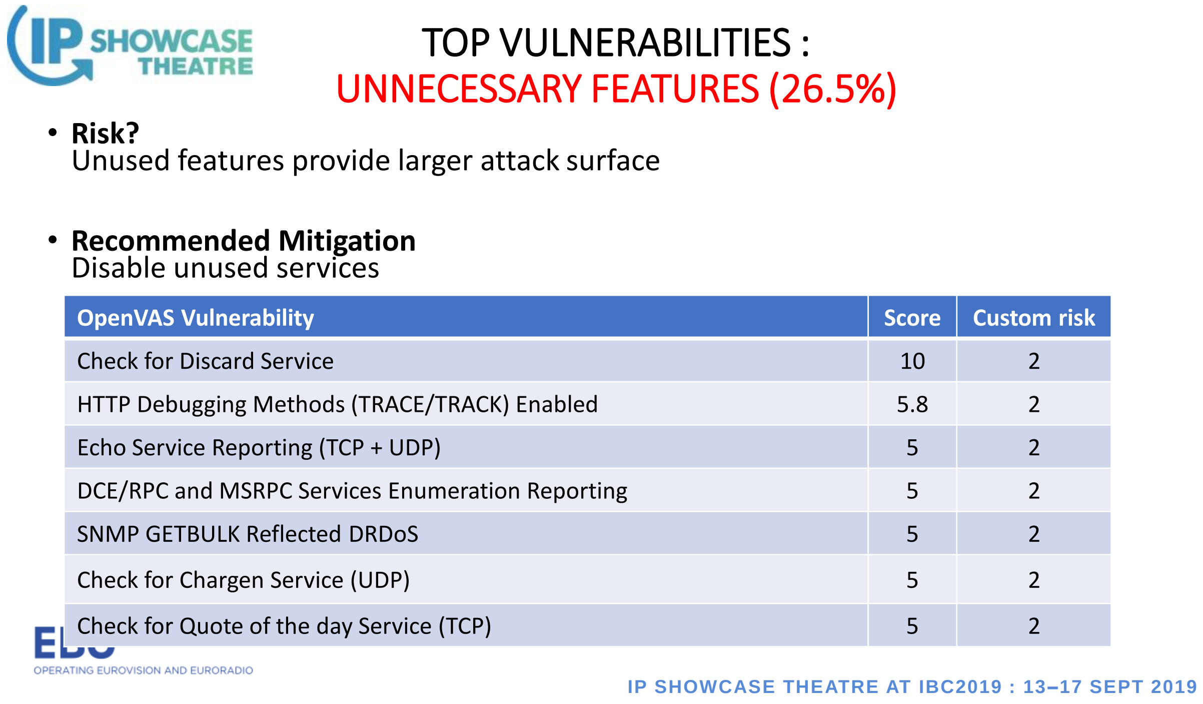
IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



TOP VULNERABILITIES : ENCRYPTION MISCONFIGURATION (33%)

OpenVAS Vulnerability	Score	Custom risk
SSL/TLS: Report 'Anonymous' Cipher Suites	5.4	1
SSL/TLS: Report 'Null' Cipher Suites	5	2
SSL/TLS: Untrusted Certificate Authorities	5	2
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5	2
SSH Weak Encryption Algorithms Supported	4.3	2
SSL/TLS: SSLv3 CBC Cipher Suites Information Disclosure (POODLE)	4.3	2
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	2
SSL/TLS: Report Weak Cipher Suites	4.3	2
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0	2
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength	4.0	2

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



TOP VULNERABILITIES : UNNECESSARY FEATURES (26.5%)

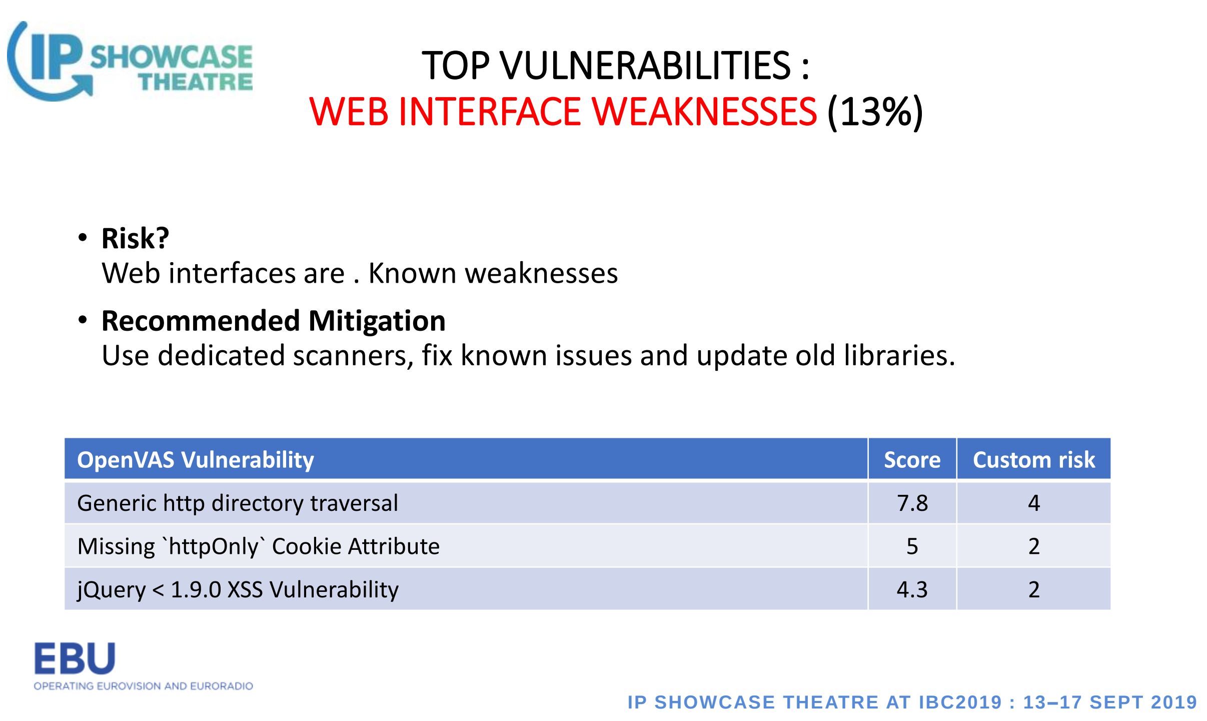
- **Risk?**
  Unused features provide larger attack surface

- **Recommended Mitigation**
  Disable unused services

OpenVAS Vulnerability	Score	Custom risk
Check for Discard Service	10	2
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8	2
Echo Service Reporting (TCP + UDP)	5	2
DCE/RPC and MSRPC Services Enumeration Reporting	5	2
SNMP GETBULK Reflected DRDoS	5	2
Check for Chargen Service (UDP)	5	2
Check for Quote of the day Service (TCP)	5	2

OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



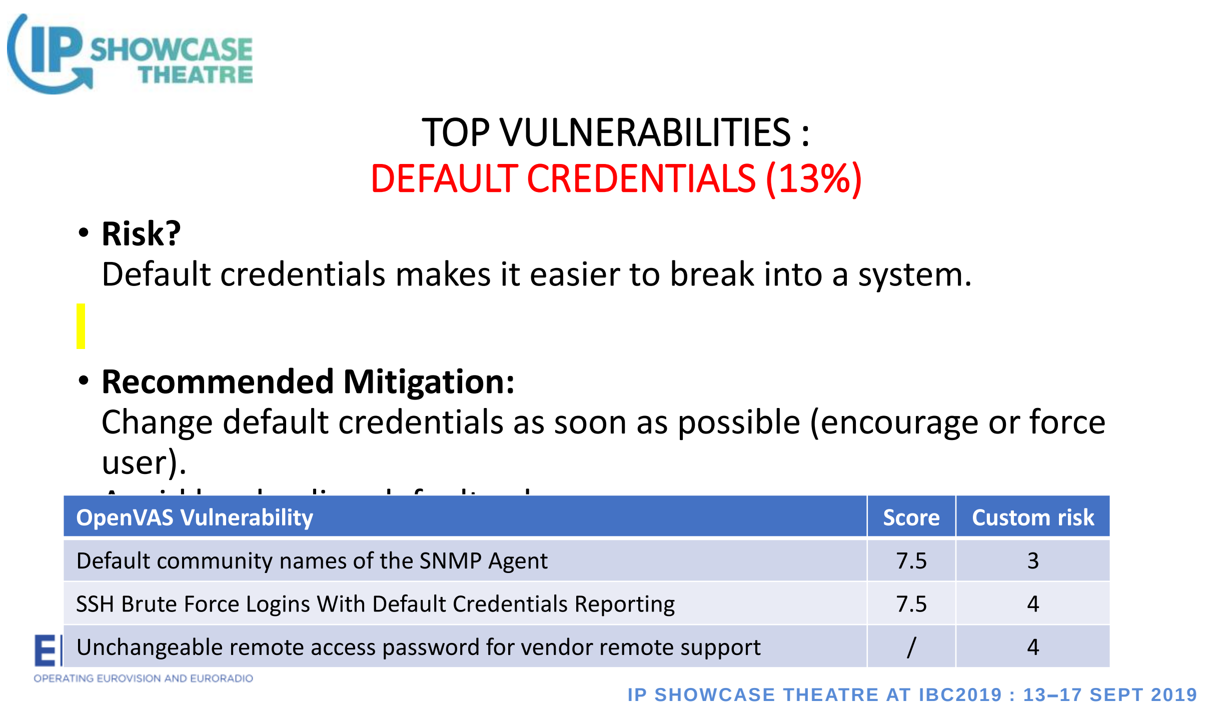
TOP VULNERABILITIES : WEB INTERFACE WEAKNESSES (13%)

- **Risk?**
  Web interfaces are . Known weaknesses
- **Recommended Mitigation**
  Use dedicated scanners, fix known issues and update old libraries.

OpenVAS Vulnerability	Score	Custom risk
Generic http directory traversal	7.8	4
Missing \`httpOnly\` Cookie Attribute	5	2
jQuery < 1.9.0 XSS Vulnerability	4.3	2

EBU
OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019



TOP VULNERABILITIES : DEFAULT CREDENTIALS (13%)

- **Risk?**
  Default credentials makes it easier to break into a system.
- **Recommended Mitigation:**
  Change default credentials as soon as possible (encourage or force user).
  [illegible]

OpenVAS Vulnerability	Score	Custom risk
Default community names of the SNMP Agent	7.5	3
SSH Brute Force Logins With Default Credentials Reporting	7.5	4
Unchangeable remote access password for vendor remote support	/	4

OPERATING EUROVISION AND EURORADIO

IP SHOWCASE THEATRE AT IBC2019 : 13–17 SEPT 2019

IP SHOWCASE THEATRE

Thank you

Gerben Dierick (VRT) - Gerben.dierick@vrt.be
Alvaro Martin (RTVE) - Alvaro.martin@rtve.se
Adi Kouadio (EBU) – Kouadio@ebu.ch

Thank you to our Media Partners

SVG SPORTS VIDEO GROUP

SVG SPORTS VIDEO GROUP EUROPE

THE BROADCAST BRIDGE Connecting IT to Broadcast

TVBEUROPE Intelligence for the media & entertainment industry

EBU OPERATING EUROVISION AND EURORADIO