EBU
OPERATING EUROVISION AND EURORADIO

JT-NM

JT-NM
Cybersecurity Vulnerability Assessment

JT-NM Tested Event August 2019, Wuppertal (Germany).

General Report

Adi Kouadio (EBU)
Gerben Dierick (VRT)
Alvaro Martin Santos (RTVE)

February 2020

L'Ancienne-Route 17A
1218 Le Grand-Saconnex (Switzerland)

Tel. +41(0)22 717 21 11
Email: tech@ebu.ch
http://tech.ebu.ch www.ebu.ch

EBU

OPERATING EUROVISION AND EURORADIO

JT-NM

L'Ancienne-Route 17A
1218 Le Grand-Saconnex (Switzerland)

Tel. +41(0)22 717 21 11
Email: tech@ebu.ch
http://tech.ebu.ch www.ebu.ch

CONTENT

L'Ancienne-Route 17A
1218 Le Grand-Saconnex (Switzerland)

Tel. +41(0)22 717 21 11
Email: tech@ebu.ch
http://tech.ebu.ch www.ebu.ch

INTRODUCTION

During the August 2019 JT-NM Tested event, a security vulnerability assessment was conducted by an expert team of the EBU Media cybersecurity (MCS) Team. The overall goal of the assessment was to educate suppliers regarding vulnerability assessment and mitigation techniques, in the hope that this will encourage them to perform self-assessments in accordance with the methods and tools given in EBU R148[1]. Such testing should be integrated throughout the product development and end-user acceptance process, providing hardened final products to the media companies. This effort underlines the importance of cybersecurity for JT-NM and its founding members (EBU, AMWA, SMPTE and VSF), who sponsor the JT-NM Tested events.

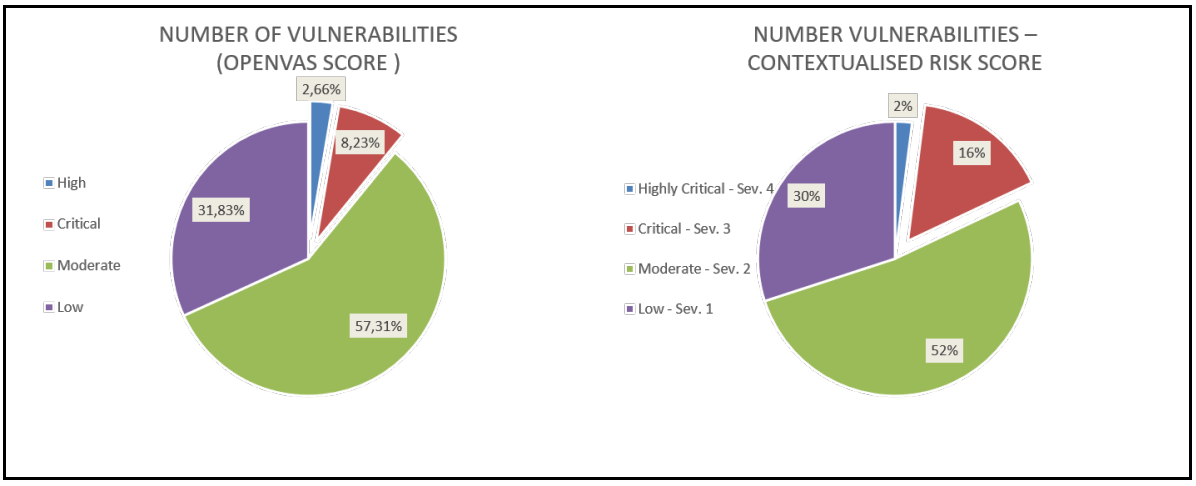
This document highlights the general findings and recommendations of the assessment.

In addition to this document, the 34 companies participating companies receive a short report highlighting the specific vulnerabilities found in their products, together with suggestions on how to mitigate the vulnerabilities that were identified during testing. We identified six vendors with devices that exhibited highly critical vulnerabilities The EBU Cybersecurity team works closely with the concerned companies to mitigate the issues.

METHODOLOGY

As a starting point, an unauthenticated vulnerability scan was performed on the different subnets of the test network using the OpenVAS open source vulnerability scanner from a Kali Linux machine.[2] The scan inspected all 65535 TCP ports and the 100 most commonly used UDP ports, using the network vulnerability tests (NVTs) available in the freely available vulnerability feed on August 18, 2019.

The scan resulted in more than **385 vulnerabilities found** across the tested devices. The scanner assigned a severity level and reliability score to each detection. The vulnerabilities were evaluated manually by cybersecurity experts to eliminate false positives and to review the severity levels assigned during automated scanning. When appropriate, vulnerabilities were verified, and risk scores were increased or decreased. As a result of this re-assessment, the number of vulnerabilities classified as critical was increased from 8% to **16%** (see figure 1).



1 http://tech.ebu.ch/pubications/r148

2 See www.openvas.org and www.kali.org

Figure 1 : OpenVAS Severity Score VS Contextualized Severity Score by EBU Cybersecurity Experts.

To improve the interpretation of the scan results, a short questionnaire was sent to the test participants. The submitted answers helped, but the team did not receive enough answers to provide useful general statistics.

RESULTS & FINDINGS

Vulnerability Categories

We have grouped the 387 discovered vulnerabilities in categories (default credentials, absence of Encryption, Encryption misconfiguration, web interface weaknesses, unauthenticated remote access, unnecessary features, unpatched software) as described in figure 2 below.

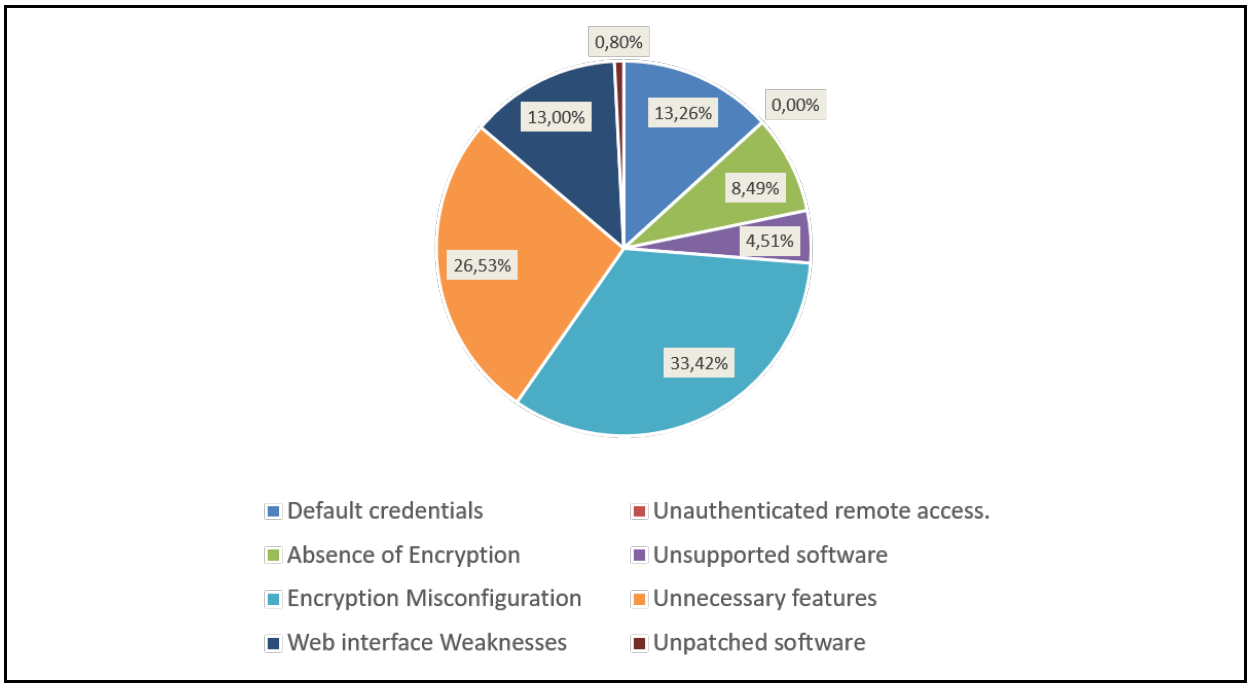


Figure 2: Percentage of occurrence of a vulnerability category as a percentage of the total number of detected vulnerabilities.

Each category is further detailed in the sections below.

1. Default credentials

Since default credentials are easily obtained from documentation or online databases, they are useless for authentication. The test setup did not allow us to verify if any of the tested systems force the user to set up a different password during the installation procedure. Only few of the vendors who answered the questionnaire indicated their systems forced changing the default password.

Some systems contained hardcoded credentials to be used for remote support by the vendors. We consider this a high risk, because these credentials cannot be changed or revoked when they are no longer secret. Possible scenarios for the disclosure of such passwords include accidental disclosure by employees, intentional disclosure by disgruntled employees and extraction from

firmware images or running systems. During the security assessment, **we were able to obtain several such passwords**.

VULNERABILITIES	SEVERITY SCORE (OpenVAS / Custom)
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.	(NS /4)

Table 1: Default Credentials - Vulnerabilities Detailed List.

2. Unauthenticated remote access

Several of the inspected systems allow unauthenticated access over the network to anybody, without any authentication. We have observed unauthenticated remote access using telnet, FTP, HTTP and HTTPS.

The severity of this vulnerability depends, of course, on the level and type of access granted to the unauthenticated user. For example, the security of the system does not necessarily suffer from a web interface which only displays some information about the system, or from anonymous FTP access that is limited to a carefully restricted part of the file system.

However, we identified several web interfaces which allowed anybody with network access to reconfigure, restart or shut down the system.

On one device, we were able to access the entire file system through anonymous FTP. This allowed access to the password hashes, which subsequently resulted in granting full access to the system after retrieving the system root password through an offline brute force attack.

The answers to the supplier questionnaire confirmed our suspicion that some participants disabled authentication on purpose to allow for easy access during test preparations. We feel that being able to disable authentication is a serious security risk. Customers may disable authentication during initial installation and never re-enable it. A secure system should prevent the user from creating a dangerous situation, by forcing a correct security setup and refusing to operate with default passwords, easy passwords or no passwords at all.

VULNERABILITIES	SEVERITY SCORE (OpenVAS / Custom)
Anonymous FTP Login Reporting	(6,4/3)
Web interface without authentication	(NS/4)

Table 2: Unauthenticated remote access – Vulnerabilities detailed list & score.

3. Unsupported software or software with known vulnerabilities

When using third party software, it is important to follow up on reported security issues. This includes moving off from older, unsupported versions, and promptly installing updates and security patches on more current versions.

Several of the devices under test were running obsolete operating systems or included software with known vulnerabilities.

VULNERABILITIES	SEVERITY SCORE (OpenVAS / Custom)
Mongoose < 6.15 Buffer Overflow Vulnerability	
Acme thttpd and mini_httpd Terminal Escape Sequence in Logs Command Injection Vulnerability	(5/2)
OS End of Life Detection	(10/3)

Table 3: Unsupported software category - Vulnerabilities detailed list & score.

4. Absence of encryption

Encryption should be used when transmitting credentials or other sensitive data, but we recommend encrypting all communications. You never know what sort of communications may contain important clues that enable an attack. Many of the systems under test sent authentication information “in the clear” using unencrypted protocols such as HTTP, Telnet or FTP. Highly secure alternatives exist for each of these protocols. We recommend disabling unencrypted access, and using encrypted alternatives such as HTTPS, SSH and FTPS.

VULNERABILITIES	SEVERITY SCORE (OpenVAS / Custom)
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)

Table 4: Absence of Encryption - Vulnerabilities list details & score.

5. Encryption misconfiguration

The vulnerability scanner reported many issues with encryption configuration or with the implementation of encryption on the systems which did provide encrypted communication. These vulnerabilities weakened the encryption in use, but in most cases, it was still enough to thwart many potential attackers.

VULNERABILITIES	SEVERITY SCORE (OpenVAS / Custom)
SSL/TLS: Report 'Anonymous' Cipher Suites.	(5.4/2)
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 Protocol CBC Cipher Suites Information Disclosure Vulnerability (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	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	

Table 5: Encryption Misconfiguration - Vulnerabilities detailed list & score.

6. Unnecessary features

Any unused software components or features cause unnecessary risks; they needlessly increase the attack surface of the system.

VULNERABILITIES	**SEVERITY SCORE (OpenVAS / Custom)**
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)	

Table 6: Unnecessary features - vulnerability list.

7. Web interface weaknesses

Many broadcast systems provide a web interface for monitoring or configuration. This means vendors must follow web application security best practices. Unfortunately, several of the systems under test contained vulnerabilities in their web interface. Some of these issues allowed access to any file on the system from the web interface. This could lead to further exploitation because it allows an attacker to steal sensitive files, e.g. files containing passwords or password hashes.

VULNERABILITIES	**SEVERITY SCORE (OpenVAS / Custom)**
Generic http directory traversal	(7.8/3 or 4)
Missing `httpOnly` Cookie Attribute	(5/2)
jQuery < 1.9.0 XSS Vulnerability	

Table 7: Web interface weaknesses - vulnerability detailed list & scores.

BROADCAST INDUSTRY SECURITY POSTURE

Before listing our recommendations for the broadcast industry, we would like to address common arguments against making products secure. Frequently this is expressed as, *"Our product is always placed in a closed network." Or "This device should not be connected to the internet." But vendors know, or should know, that it is rarely the case that broadcast equipment operates entirely without any connection to the outside world.*

Even if the device is not accessible from the internet, in almost all cases the broadcast network will have some sort of connection with the user's business network. Also, one strong incentive to adopt computer technology in media facilities is the ability to remotely operate and troubleshoot systems. Does it really make sense for suppliers to assume the devices will be perfectly isolated? In fact, several vendors require remote access to broadcast systems through internet in order to fulfil their support contracts. This level of access shall come with an obligation on the vendor to provide a secure system at first. Vendors should not force or trust their customers to shield their products from possible threats but should **provide the customer with hardened systems in the first place**.

Another popular argument, heard in many variations, is the idea that broadcast equipment is not an interesting or attractive target for an attacker *e.g. "Why would anybody attack this type of device?"*. This is incorrect for two reasons.

First, lots of attackers do not care what type of device they are dealing with, or don't even know. Most of the tested broadcast devices are simply computers, running well known operating systems and common network services. An attacker scanning a network will see a vulnerability on some IP address, and will exploit it without knowing he is dealing with broadcast equipment. Even if no direct damage can be done on such a system, it could serve as a starting point for further attacks on connected devices, even if they are inaccessible from the outside.

Second, in fact, broadcasters and other media outlets are an interesting target for several reasons. They are well known and have a lot of visibility. Broadcasted content can also antagonise groups of people or organisations and trigger malicious activity.

To lower these risks, equipment suppliers need to do their part and provide secure products that form a part of the overall secure broadcasting infrastructure.

GENERAL RECOMMENDATIONS

We expect all vendors to investigate the risks caused by all exploitable vulnerabilities identified during the scans, and fix or otherwise mitigate when appropriate. EBU MCS will follow up with suppliers for products found to have critical vulnerabilities, following the procedure described in EBU R160.

All vendors should, at a minimum, publish a security contact procedure for reporting security issues to them. We recommend vendors publish a full responsible disclosure policy outlining how security researchers can cooperate with them. For inspiration on such a policy, please refer to EBU recommendation R161.

The basic security scan, as performed during the JT-NM Tested event, requires limited time and can be performed using freely available open source tools. This allows suppliers to regularly run scans on their own products. EBU recommendation R148 lists several additional tests which should be part of such a self-assessment. Even if the interpretation or verification of some of the results may require assistance from security experts, regularly running the scans will warn the product development team of new issues being introduced.

New broadcast systems are built using common IT hardware and software. Gone are the days when broadcast equipment consisted of custom software running on dedicated hardware. This is a logical evolution, and vendors must adopt best practices from the IT industry, especially best practices on cybersecurity, even if this requires specialized training for product teams.

CONCLUSION

We are grateful to all the vendors that participated in the assessment. The open, cooperative spirit has raised the industry's awareness of cybersecurity and has demonstrated that manufacturers and users can work together to improve the security of IT-based media facilities.

Vendors with critical vulnerabilities have been pro-active in collaborating with EBU MCS to remedy the vulnerabilities in due course, in accordance with EBU R160.

For the next JT-NM interop test (Houston March 2020 and beyond), vendors are expected to run their own EBU R148 test. The goal of the EBU MCS is to help the industry raise its security maturity level, and therefore, it will continue to support the JT-NM Tested events with cybersecurity vulnerability assessments.