EBU

OPERATING EUROVISION AND EURORADIO

R 148

CYBERSECURITY RECOMMENDATION ON MINIMUM SECURITY TESTS FOR NETWORKED MEDIA EQUIPMENT

RECOMMENDATION

Geneva
April 2018

This page and others in the document are intentionally left blank to maintain pagination for two sided printing

Cybersecurity Recommendation on minimum security tests for networked media equipment

EBU Committee	*First Issued*	*Revised*	*Re-issued*
TC	2018		

Keywords: Security, Testing, Infrastructure, Broadcasting, IP.

Recommendation

The EBU, considering that,

1. Production workflows and infrastructures are rapidly migrating to generic IT technologies.
2. Connected media devices still tend to have a low security threshold inherited from the era of non-connected broadcast media where cybersecurity due diligence was often not a top priority for manufacturers and users.
3. Media companies increasingly employ third parties to provision their systems, software and services.
4. Cyberthreats (e.g. malware and ransomware) are increasingly easier to perform and are continuously evolving.

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.

Annex: Recommended minimum Security tests

TEST NAME	OBJECTIVES	METHODOLOGY	EXAMPLE TOOLS	EXPECTED OUTCOME	SCORE / REPORTING
⑩ CHECK EXPLOIT DATABASES	Does the device have documented known vulnerabilities in certain software versions and has the vendor patched these?	Check the current firmware version of the device. Check sites with well-known vulnerabilities for the vendor name and version.	https://www.exploit-db.com/	All the possible known vulnerabilities.	List the number of known vulnerabilities
			https://www.securityfocus.com/vulnerabilities		Is this device shipped with the patched software preinstalled?
			Vendor specific vulnerability database (if available).		
① PORT SCAN	Verify that NO unauthorized ports are open for remote communication.	Performing a full TCP and UDP connect scan on the IP address of all IP interfaces of the device.	Nmap - https://nmap.org/	All the open TCP and UDP ports with services behind it.	**PASS:** Port is open and documented by the vendor
			https://github.com/nccgroup/port-scan-automation		**FAIL:** Port is open and not documented
			https://github.com/robertdavidgraham/masscan		Comment on open ports.
② VULNERABILITY SCAN	Verify that there are no missing patches, weak passwords, mis-configurations , XSS, etc. on OS, System, and Application-Level.	Scanning all IP interfaces on the network level, enumerate the services and check for vulnerabilities at system and application level (arachni).	**SYSTEM LEVEL**	Vulnerability Findings.	Severity
			Nessus - https://www.tenable.com/products/nessus/nessus-professional		Count
			Nexpose - https://www.rapid7.com/products/nexpose/		
			Open-VAS - http://www.openvas.org/		
			SYSTEM AND APPLICATION LEVEL		
			arachni (web-front-end) - http://www.arachni-scanner.com/		
③ WEB SERVER VULNERABILITY SCAN	Finds common vulnerabilities related to web server configuration and specific web application issues.	Use scanning tools to check for XSS possibilities, session management errors, wrong use of headers, SQL injection attacks and other OWASP Top 10 vulnerabilities.	OWASP ZAP https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	All possible vulnerabilities on the (management) web portal	Number of vulnerabilities
			Burp Suite - https://portswigger.net/burp		
			Arachni - http://www.arachni-scanner.com/		

Cont.

TEST NAME	OBJECTIVES	METHODOLOGY	EXAMPLE TOOLS	EXPECTED OUTCOME	SCORE / REPORTING
④ FUZZING	**PROTOCOL FUZZING**				
	PROTOCOL FUZZING: Create malcrafted packages to provoke unexpected behaviour.	Protocol fuzzing is done by crafting malicious packages that are not handled correctly by the device causing an unexpected behaviour (e.g. DOS of device).	American fuzzy lop - http://lcamtuf.coredump.cx/afl/ Scapy - http://www.secdev.org/projects/scapy/ OpenRCE sulley - https://github.com/OpenRCE/sulley	**Protocol Fuzzing:** The device creates debugging information logs and is resilient against DOS.	**Protocol Fuzzing:** The device is reacting as expected.
	URL FUZZING				
	URL FUZZING : Find hidden files and directories on the (management) web portal on the device.	URL fuzzing is a discovery activity which allows you to discover resources that were not meant to be publicly accessible (ex. /backups, /index.php.old, /archive.tgz, /source_code.zip, etc). Since 'security by obscurity' is not a good practice, we can often find sensitive information in the hidden locations identified by the URL Fuzzer.	URL fuzzer American fuzzy lop Dirbuster - https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project Gobuster - https://github.com/OJ/gobuster Nikto - https://cirt.net/Nikto2 OpenRCE sulley	**URL Fuzzing:** All hidden web directories or files that might threaten the confidentiality, integrity or availability of the device/ service.	**URL Fuzzing:** All web directories and file with comments on files that may threaten the device.

Cont.

TEST NAME	OBJECTIVES	METHODOLOGY	EXAMPLE TOOLS	EXPECTED OUTCOME	SCORE / REPORTING
Ⓢ PASSWORD (CREDENTIALS PROTECTION)	Are users forced to change default passwords during install?	Manual setup of the device from the factory default.	Burp Suite		Answers to the questions in the objective.
	Is it possible to use a simple password?	Check if passwords have to be changed.	Manual testing		
	Are there any hard-coded passwords?	Check if default passwords can be used after changing the password.			
	Are passwords securely protected?	Possibly try brute-force using well known passwords.	**AUTOMATED BRUTE-FORCE**		
			Hydra - http://sectools.org/tool/hydra/		
			Medusa - https://github.com/jmk-foofus/medusa		
			Ncrack - https://nmap.org/ncrack/		
			John the Ripper - http://www.openwall.com/john/		
			hashcat - https://hashcat.net/hashcat/		
			ophcrack / rainbowtable -		
Ⓖ PTP (Precision Time Protocol)	Do PTP slaves have adequate protection against rogue masters and denial of service attacks?	Start a PTP master next to another PTP master and observe the reaction. Use IP / MAC address spoofing - Give a system the same IP address as the Master and observe how the devices react. What happens if the PTP master is flooded with packets (DoS). observe reaction.	Manual set up.	PTP slaves should have adequate protection against rogue masters and denial of service attacks.	Answers to the questions in the objective.

Cont.

TEST NAME	OBJECTIVES	METHODOLOGY	EXAMPLE TOOLS	EXPECTED OUTCOME	SCORE / REPORTING
⑦ LOG MANAGEMENT	Logs are timestamped and secured to enable audit of evidence. Also make sure the logs contain useful information.	Check the logfiles after tests 1-5 to see if attacks are actually visible in the logs.	Tail / grep commands Manual check	Logfiles with all the information	Answers to the questions in the objective.
⑧ FIRMWARE & OS	Is the firmware / OS up to date? And are the latest security updates installed? Is the Firmware itself secure?	Set up the device and check management settings for upgrade possibilities. Check the vendor support website for updates and changelogs. Run security test against firmware	Vendor website for latest firmware version. IDA Debugger (HEX-rays) to check if the firmware itself is secure.		Answers to the questions in the objective.
⑨ INTEGRATION WITH EXTERNAL SERVICES	Are the device's security functions stand-alone or can they be integrated with external services, such as secure LDAP / SAML / AD integration and/or SYSLOG export etc?	Set up the device and check management settings for integration possibilities.	Manual check		List of possibilities to integrate with external services.
⑩ NETWORK COMMUNICATION ORIGINATING FROM DEVICE	Is the device broadcasting information about itself? Is the device 'calling home' to the vendor in a certain interval?	Connect the device to a SPAN or mirror network port and capture the network traffic originating from the device	Wireshark Tshark Tcpdump		Answers to the questions in the objective.

Cont.

TEST NAME	OBJECTIVES	METHODOLOGY	EXAMPLE TOOLS	EXPECTED OUTCOME	SCORE / REPORTING
⑪ MANAGEMENT INTERFACE PROTECTION	Is the management interface protected (e.g. password, https) and separated from the data interface.	Perform a vulnerability scan. Check the interface seperation. Manual verification of the configuration.	See row #02 - vulnerability scan tools.		the management interface is protected (e.g. password, https) and separated from the data interface.