EBU

OPERATING EUROVISION AND EURORADIO

R 160

VULNERABILITY MANAGEMENT PROCEDURE TOWARD MEDIA EQUIPMENT VENDORS

SOURCE: Media Cybersecurity Group

Geneva
June 2019

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

Vulnerability Management Procedure
Toward Media Equipment Vendors

EBU Committee	*First Issued*	*Revised*	*Re-issued*
TC	2019		

Keywords: Vulnerability disclosure, Vulnerability management, Media system vendors, hackers, risk assessment.

The EBU recommends that media companies[1] confronted with critical vulnerabilities in their media equipment adopt the following procedure to establish a fruitful collaboration with the concerned system vendor(s).

The procedure is designed to allow enough time for media system vendors to respond to a media company's inquiry and its overall goal is to foster a constructive dialogue between vendors and media companies, leading toward a more secure media industry overall.

PROCEDURE

STEP 1: A media company detects one or several critical security vulnerabilities in a product or service and discloses these to the EBU in the form of a security audit report.

A critical vulnerability is one that has a high potential/probability of being exploited to harm the media company (e.g. any high impact incident such as take control of devices or infrastructures, endangers services, steal credentials, etc.). It is assumed that the media company would have done its due diligence i.e. a risk assessment of the vulnerability discovered before they communicate with the vendor or the EBU.

The media company notifies the vendor about the vulnerability, making it clear that the communication is governed by EBU R160 procedure. If the vendor has a responsible disclosure policy, this channel is the preferred means of notification. If this is unavailable, the media company is encouraged to establish contact with the vendor through any other means.

Expectations:

Vendors are required to provide the media company with a satisfactory response including a detailed remediation plan within 60 days from notification date.

STEP 2: If a satisfactory response has not been received from the vendor within 60 days, the EBU is informed and it issues an official letter to the vendor detailing the following:

- Identified vulnerabilities to be fixed.
- Risk assessment of the vulnerability.
- Description of the different potential abuse scenarios.

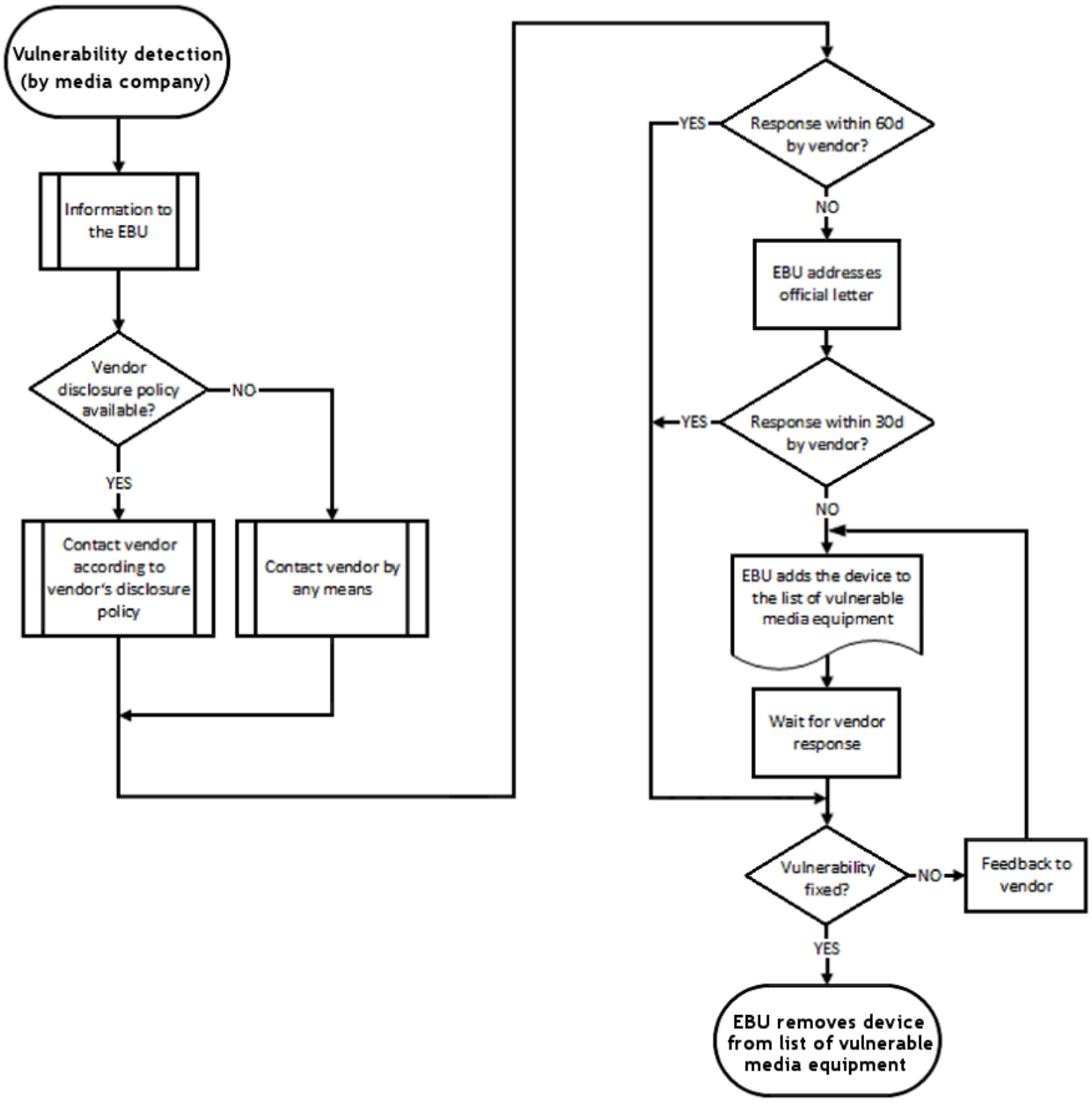
[1] Media companies include EBU Members & other broadcasters, their production partners & other content providers.

Expectations:

Response from the vendor within 30 days (following prior notification from the media company) or 90 days (if a first notification) regarding the outlined issues including a detailed remediation plan.

STEP 3: If no satisfactory response has been received from the vendor, the EBU will update a published list of critical media vendor systems. This list will document the device name, the vendor, as well as other relevant identification details (firmware version, etc…).

STEP 4: The list will be updated again 90 days after an issue has been confirmed as remediated.



EBU's Vulnerability Management Procedure Workflow