EBU

OPERATING EUROVISION AND EURORADIO

# R 160

# VULNERABILITY MANAGEMENT FOR MEDIA COMPANIES AND MEDIA SYSTEM VENDORS

RECOMMENDATION

Version 2.0

Geneva
September 2023

## Document History

| | | |
|---|---|---|
| EBU Committee | TC | |
| Drafting Group | Media Cybersecurity Group (EBU MCS) | |
| First published | June 2019 | |
| Revised | Sept. 2023 | Version 2.0 –Developed in detail; recommendations to Media companies before and after Media Product purchase, and to Vendors before and after Product release, for security scans and tests and Vulnerability management. |
| | | |

**Publication Keywords:** Cybersecurity, Media Systems, Vulnerability, Vendor, Vulnerabilities, CVE, CVSS, CNA.

## Acknowledgement

EBU technical publications are the work of experts from EBU Members, Associate Members and third parties consisting of international standards bodies, industry partners, academic institutions and independent consultants.

Their contribution to EBU technical publications is a very generous act by the individuals concerned and by their employers. The EBU appreciates their efforts and thanks them most sincerely.

This report has been produced with the assistance of the following entities:

**EBU Members**: Media Cybersecurity Group.

**EBU Project Manager:** Lucille Verbaere

## *Definitions*

| | |
|---|---|
| **Media Company** | The organisation that is in the process of purchasing a Media System Product or owns a Product that may be used in production. |
| **Media Systems:** | Any Hardware device and Software running on a hardware or in the Cloud. |
| **Product:** | A Media System being provided by the Vendor to the Media Company. |
| **Vendor:** | The potential Vendor (including appointed sub-contractors) providing the Product, service, system or software. |
| **Reporting Entity** | A Reporting Entity is an entity that has performed security tests on a Product, has found a vulnerability, and that reports the vulnerability to the Media Company and/or the Vendor. For example, it could be a Media Company, EBU MCS, a Security Service Provider, or an independent security researcher. |
| **CVE ID:** | Common Vulnerabilities and Exposures identification number. A public ID that uniquely identifies a vulnerability in a certain product. More information on the CVE process can be found here: https://www.cve.org/About/Process |

| | |
|---|---|
| **CVSS:** | Common Vulnerability Scoring System. A notation and metric for assessing severity and impact of security vulnerabilities. CVSS base score is a single value used to summarize the severity of the vulnerability, whereas a CVSS vector string is a compressed textual representation of the values used to derive the CVSS base score. Specification documents and calculators can be found on SIG website: Common Vulnerability Scoring System SIG. |
| **CNA:** | CVE Numbering Authority. An entity authorized to issue CVE IDs for vulnerabilities affecting products that fall under the CNA's scope. |

## Recommendation

### *The EBU, considering that:*

1. Media companies increasingly employ third parties to provision their systems, software and services.
2. Production workflows and infrastructures are rapidly migrating to generic IT technologies and connected to Public Internet.
3. The number of Cyber-attacks against organisations, including Media Companies, has greatly increased during the past years.
4. Attackers leverage vulnerabilities in IP-based systems e.g., to introduce malware or take over control of organisations' systems.

### *Recommends that Media Companies:*

1. Make sure their technical teams develop security testing skills through regular training.
2. Publish a security contact to whom to report vulnerabilities and implement a responsible vulnerability disclosure policy such as recommended in EBU R161.
3. Share with EBU and EBU members any security-relevant findings in order to establish effective vulnerability management in the Media industry.

***Before Purchasing and deploying a Media system:***

4. Evaluate the media Vendor and their product security using the assertion sheet from EBU R143.
5. Set up the Product according to best security practices and following the security guidelines and hardening recommendations in the Product's documentation.
6. Test the Product security and verify security assertions made by the Vendor. Basic security tests could include (but are not limited to):

- Generic vulnerability scans
- Network port scans
- Password security checks
- Cryptographic protocol checks
- Isolated management interface check
- Documentation checks for device hardening techniques.

7. Subject to resource availability, perform advanced security tests against the Product. Advanced security tests could include (but are not limited to):

- Web application penetration tests
- Firmware image or code analysis
- Passive and active network traffic analysis

8. Notify the Vendor when vulnerabilities are identified and work with the Vendor to fix the issue. Follow the Vulnerability management procedure described in the Annex.
9. Do not deploy the Product until presented with an effective fix for the identified issues.

For more detailed instructions on how to conduct basic and advanced security tests, Media companies can consult the EBU's Security and Testing Guidelines. EBU Members can also benefit from EBU Academy Cybersecurity Master Classes for engineers and technicians, to further develop security testing skills within their technical teams.

***After deploying a Media system:***

1. Perform continuous generic vulnerability scans against the deployed Product throughout its lifespan in order to detect new security vulnerabilities in the Product's components and supporting systems and services.
2. Regularly monitor newly announced Product updates and follow instructions provided by the Vendor in order to ensure security and functional upgrades are timely applied to the Product.
3. Repeat the set of basic and advanced security scans before re-deploying a newly upgraded Product.
4. Follow the vulnerability management procedure described in the Annex.
5. Do not re-deploy the Product until presented with an effective fix for the identified vulnerabilities.

## *And recommends that Vendor companies:*

***Before releasing a new product or a new version of the product:***

1. Perform standard Quality and Assurance (QA) tests.
2. Perform security tests against the Product. Security tests include (and are not limited to):

- Generic vulnerability scans
- Any tests according to a relevant reference framework. For example, if the Product features a web application as part of the management interface, the Vendor should, at the very least, ensure the product is immune to all vulnerabilities from the OWASP Top 10 list.

3. Provide detailed guidelines for Media companies on how to correctly configure security parameters of the Product.
4. Publish detailed information on how to contact relevant personnel for vulnerability disclosure purposes.

***After releasing a new Product or a new version of the Product***

1. Actively monitor and apply security updates related to all components of the Product, including Operating System and third-party software.
2. Perform continuous generic vulnerability scans against the newest version of the Product in order to detect new security vulnerabilities in the Product's components, supporting systems and services and apply standard Quality and Assurance tests.

3. Act upon newly identified security vulnerabilities without delay, by warning Product users and releasing security upgrades that remediate the identified security vulnerabilities at no extra cost to Product users during the whole lifecycle of the Product.

***Upon receiving a report that a vulnerability has been detected in their Product:***

1. Follow the Vulnerability Management Procedure described in the Annex.

# ANNEX: Vulnerability Management Procedure for Media Companies and Media system Vendors

Upon identifying a vulnerability in a Product, either by means of independent testing or after receiving a vulnerability report from a Reporting Entity, the Media Company and Vendor are advised to carry out the following Vulnerability Management procedure:

## Domain of responsibility identification

Before contacting the Vendor or the EBU MCS, the Media Company should check if the identified vulnerability can be successfully resolved by applying standard configuration changes to the concerned Product. Standard configuration changes are any changes the Vendor has identified before shipping the Product and for which it has recorded accurate instructions in the Product's documentation (e.g., resetting default passwords, upgrading to secure transport protocols, deactivating unnecessary services etc.). If the vulnerability can indeed be resolved by applying standard configuration changes, the Media company should follow the instructions provided in the Product's documentation.

## Severity and impact identification:

If the vulnerability cannot be resolved by re-configuring the security parameters as instructed in the Product's documentation, the Media company should assess the severity and the impact of the vulnerability. The severity of the vulnerability should be assessed by calculating its CVSS base score and CVSS vector string. To do this, the Media Company can use the calculator available at Common Vulnerability Scoring System SIG. After obtaining the CVSS base score and CVSS vector string for the vulnerability, the Media company should assign the vulnerability to a severity group, as follows:

- Critical vulnerabilities: Any vulnerability with CVSS base score of 9.0 or greater
- High-severity vulnerabilities: Any vulnerability with CVSS base score in range [7.0, 8.9]
- Medium-severity vulnerabilities: Any vulnerability with CVSS base score in range [4.0, 6.9]
- Low-severity vulnerabilities: Any vulnerability with CVSS base score in range [0.1, 3.9]

## Vulnerability reporting:

Once the severity and impact of the vulnerability is assessed, the Media company should report the vulnerability to the Vendor providing:

- Description of the vulnerability in sufficient detail to replicate it.
- The calculated CVSS base score and CVSS vector string.

If the vulnerability has a critical severity or impact, or if the Media company suspects that the vulnerability could negatively impact other Media Companies, the Media company may notify the EBU Media Cybersecurity (EBU MCS) group.

The notification to the EBU MCS should include the following details:

- Vendor, device model and firmware version affected by the potential vulnerability.
- Description of the vulnerability type.
- The calculated CVSS base score and CVSS vector string.

## Remediation process by Media system Vendors:

Upon receiving a report that a vulnerability has been detected in their Product, the Vendor should reply to the Reporting Entity and Media Company with the following information within 8 days:

1. Acknowledgement that the vulnerability report has been received.
2. Proposal of temporary mitigation strategies that prevent the exploitation of the vulnerability.
3. An estimate when a permanent patch that completely resolves the vulnerability will be available.
4. **P**roof that a CVE ID has been requested to an appropriate CNA. The proof can take one of the following forms:
    a. CVE ID in a reserved state.
    b. In case of CVE requests that have not yet received a CVE ID reservation - a confirmation e-mail with a reference number delivered by the CNA. The Vendor should provide an update containing the reserved CVE ID as soon as it becomes available.

In case of critical vulnerabilities, the Vendor should also send the information indicated above to all other Media Companies and to the EBU MCS.

The Vendor should immediately start developing a patch that permanently resolves the vulnerability and update the mitigation strategy accordingly. In case of critical vulnerabilities, the Vendor should keep all Media Companies and the EBU MCS regularly updated on the status of current patch developments. The Vendor is expected to develop an effective patch within 3 months after receiving the initial report of the vulnerability and proactively look for support from Media Companies and the EBU MCS if needed.

Once a permanent patch has been finalized, the Vendor should notify all Media Companies. The notification should state what vulnerability is being resolved and clearly communicate how time-critical it is for Media Companies to apply the new patch. In case the patch resolves a critical vulnerability, the Vendor should also notify the EBU MCS.

Finally, the Vendor should work with the responsible CNA on making the previously reserved CVE ID public. Once this process completes, the Vendor should notify all Media Companies and, in case of critical vulnerabilities, the EBU MCS.

**If the Vendor does not follow the process and timelines given above, the Reporting Entity and Media Company should contact the EBU MCS, that can:**

- **Contact the Vendor.**
- **Add the Product to an internal list of vulnerable Products.**
- **Engage, together with the Media Company and Reporting Entity, an appropriate CNA in the CVE ID reservation and publication process.**
- **Notify all EBU Members.**
- **Notify other Broadcasting Unions or publicise the issue ('go public').**

**If a vulnerability is being actively exploited, the Vendor should act without delay to notify their customers. This communication should include immediate mitigation strategies. In such circumstances, the EBU will not adhere to the above timelines and will itself act as it sees fit to notify its Members of the potential risks.**