EBU

OPERATING EUROVISION AND EURORADIO

Responsible Vulnerability Disclosure Policy

October 2020

Version 1.1

EBU

OPERATING EUROVISION AND EURORADIO

Contents

Context

The EBU (European Broadcasting Union) considers important that its information and systems are secure. Despite our concern for the security of these systems, it may occur that there are still some potential vulnerabilities.

The EBU is grateful for investigative work into security vulnerabilities which is carried out by well-intentioned, ethical security researchers. We are committed to thoroughly investigating and resolving security issues in our platform and services in collaboration with the security community.

This document aims to define a methodology by which the EBU can work with the security research community to improve EBU's online security.

Scope

We are interested in hearing about critical security issues on the following scope. If you find a vulnerability on an unlisted domain or scope, we advise you to produce beforehand a short vulnerability report before going to deeply into an analysis so that we can answer you about its validity and criticality.

If you report a vulnerability that our teams are already aware of, we will inform you about it straightforward.

The information you will provide us will most of the time allow us to analyze and draw conclusions on the vulnerability potential impact.

To be eligible to our Hall of Fame, we typically require the issue report to have some actual and critical security impact in a realistic scenario and does not mean you need to solve the issues.

Currently, the scope of our vulnerability disclosure program is limited to certain vulnerabilities. However, we are happy to thank everyone who submits a non-high-severity vulnerability".

In scope

This disclosure policy applies only to vulnerabilities in EBU's products and services under the following conditions:

- Vulnerabilities which are original and previously unreported and not already discovered by internal procedures
- Domains **ebu.ch** and **eurovision.net** and their **subdomains**.

Out of Scope

Any services hosted by third party(ies) providers and services are excluded from scope.

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following vulnerabilities types are excluded from the scope of this policy:

- Volumetric vulnerabilities (i.e. simply overwhelming our service with a high volume of requests).
- TLS configuration weaknesses (e.g. "weak" ciphersuite support, TLS1.0 support, sweet32, etc.)
- Network level Denial of Service (DoS/DDoS) vulnerabilities
- Reports indicating that our services do not fully align with "best practice" e.g. missing security headers (e.g. CSP, x-frame-options, x-prevent-xss, etc.) or suboptimal email related configuration (e.g. SPF, DMARC, etc.)

Never attempt non-technical attacks such as social engineering, phishing or physical attacks.

Reporting a vulnerability

If you discover a vulnerability in one of our systems, we ask you to:

- Report the vulnerability as soon as possible after discovery. Mail your encrypted findings to vulnerability@ebu.ch or enter them directly into our *vulnerability reporting form* using the link: https://www.ebu.ch/about/contact-us/vulnerability-disclosure
- Provide sufficient information to reproduce the vulnerability so that we can solve the problem as quickly as possible. Usually the IP address or URL of the affected system and a description of the vulnerability is sufficient, but for more complex vulnerabilities more information may be needed.
- Leave your contact details, so that the EBU can contact you to work together for a safe result. Leave at least your name, e-mail address and/or other contact information. Reporting under a pseudonym is however possible, but make sure that we are able to contact you should we have additional questions.
- Confirm your action and that you will continue to act in accordance with this Responsible Disclosure Policy.
- We may choose to ignore low quality information reports.

Guidance

Security researchers must not:

- Access unnecessary amounts of data. For example, 2 or 3 records are enough to demonstrate most vulnerabilities (such as an enumeration or direct object reference vulnerability);
- Violate the privacy of EBU users, staff, contractors, suppliers, etc. For example, by sharing, redistributing and/or not properly securing (personal) data retrieved from our systems or services;
- Communicate any vulnerabilities or associated details via methods not described in this policy or with anyone other than your dedicated EBU security contact;
- Modify data in our systems/services which is not your own;
- Disrupt our service(s) and/or systems; or
- Disclose any vulnerabilities of the EBU systems/services to third parties/the public prior to the EBU confirming that those vulnerabilities have been mitigated or rectified.

We request that any and all data retrieved during research is securely deleted as soon as it is no longer required and at most, 1 month after the vulnerability is resolved, whichever occurs soonest.

Any action undertaken by a security researcher under this Responsible Disclosure Policy should be limited to conducting tests to identify potential vulnerabilities and sharing this information with the EBU.

Hall of Fame

Unfortunately, due to the EBU's funding structure, it is not currently possible for us to offer a paid bug bounty program. We would, however, like to thank the security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy.
The name of reporters of qualifying vulnerabilities will be display on our “Hall of Fame”

Legal Framework

This policy is designed to be compatible with common good practice among well-intentioned security researchers. It does not give you permission to act in any manner that is inconsistent with the law or cause the EBU to be in breach of any of its legal obligations as well as EBU internal policies, including but not limited to:

- The EU General Data Protection Regulation 2016/679/ EU (GDPR)
- Swiss Data Protection laws and regulations including the Swiss Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 March 2019)

The EBU will not seek prosecution of any security researcher who reports in good faith and in accordance with this policy, any security vulnerability on an in-scope EBU and ESSA services.

Feedback

If you wish to provide feedback or suggestions on this policy, please contact our security team: vulnerability@ebu.ch. This policy will evolve over time and your input will be valued to ensure that it is clear, complete and remains relevant.

We reserve the right to change the content of this Policy at any time, or to terminate the Policy.