EBU
OPERATING EUROVISION AND EURORADIO

R 161

RESPONSIBLE VULNERABILITY DISCLOSURE PROGRAMME FOR MEDIA COMPANIES

SOURCE: Media Cybersecurity Group

Geneva
July 2019

Abstract

With increasing levels of cyberthreat on the internet, media organisations must adopt new techniques to mitigate security risks. With increases in software development and application deployment, tracking and assessing the security of large numbers of applications are becoming difficult. One successful pre-emptive approach to vulnerability mitigation is the establishment of a responsible disclosure programme or policy.

By detailing the permitted scope of any testing and the process by which bugs and vulnerabilities can be reported it is hoped that the security research community will be encouraged to investigate and disclose issues responsibly before they can be exploited. This recommendation provides guidance for media companies on how to establish such vulnerability disclosure policies and programmes. It also proposes an example policy which can be customized to the organisation's own policies, processes and legal framework(s).

This policy does not preclude, or make any specific recommendations regarding the use of brokers to administer responsible disclosure programmes or reward programmes ('bug bounty' programmes) and these may also be worth considering, especially in lack of skilled security personnel.

Contents

Responsible Vulnerability Disclosure Programme for Media Companies

EBU Committee	First Issued	Revised	Re-issued
TC	2019		

Keywords: Bug bounty, responsible disclosure policy, hackers, white hats, vulnerability disclosure, security researchers

Recommendation

The EBU, considering that:

- Organisations are increasingly vulnerable to cyberattacks, especially those targeting web applications.
- Media organisations rely extensively on continuous application development and deployment for their media services.
- Organisations in other industries successfully crowdsource their vulnerability assessment tasks to efficiently complement their own vulnerability assessment processes.

Recommends that:

Every media company shall establish **a responsible vulnerability disclosure programme (RVDP)**. The responsible disclosure process can be implemented directly by the media company if it has the relevant security team to handle the submissions in due time. Otherwise, the whole process can be outsourced to a vulnerability assessment broker.

In either case, the media company shall publicly advertise the availability of such a responsible disclosure programme, clearly indicating means and policies for security researchers to submit their findings.

For both cases, the following items shall be implemented:

1. An online **description of the vulnerability disclosure programme**, outlining:

   - **When internal,** The **Vulnerability Disclosure Policy** (rules to follow and expectations for submissions) in case of a vulnerability disclosure. This includes a dedicated secured and monitored communications channel for vulnerability disclosure (e.g. an e-mail address such as security@mediacompany.com) managed by the relevant internal team. All email exchanged between the researcher and the company should be secured by an encryption mechanism such as PGP.

     Annex A provides a checklist and describes the main structure of a vulnerability disclosure policy. An example of vulnerability disclosure policy is available in *Annex B*. Media companies are encouraged to use it as an inspiration to create their own.
   - **When outsourced,** a short description of the vulnerability disclosure programme managed by the broker, including a link to the broker website.

2. An **Acknowledgement web page** for the security researchers that have had successful vulnerability submissions and the severity of the vulnerability. The acknowledgement can be ordered per vulnerability criticality and year.

Annex A: Responsible Vulnerability Disclosure Programme Checklist

The following checklist is intended to verify that the media company has defined and established all the necessary elements of an effective vulnerability disclosure programme.

The media company should verify that:

1. The vulnerability disclosure policy is online and up to date with each of the following sections described:

   - **Scope**: This section should describe the type of service you authorise for external vulnerability assessment.
   - **Out of Scope**: This section should describe the type of service that are not considered relevant for external vulnerability assessment as well as vulnerability submissions that are not considered for reward.
   - **Rewards**: This section should describe the type of reward your company proposes for the categories of vulnerability considered.
   - **Rules**: This section describes the rules and limitations within which the researcher can conduct his investigation on the media company's services and assets.
   - **Reporting a vulnerability**: This section describes how to submit a vulnerability and what should be included in the submission.
   - **Process\What to expect**: This section describes the management procedure for any vulnerability submission.
   - **Legal Framework:** This section describes the laws and regulations under which the researcher must conduct his investigation. The listed laws usually match the country's legal regulation around cybercrime and data protection.

2. The policy has been reviewed and approved by its internal legal department.

3. The secured contact e-mail address / messaging systems is available and monitored and advertised online. (PGP Public KEY or other means of receiving encrypted mail).

4. The internal Security Team is responsible to follow up on the disclosures.

5. The Acknowledgement page for Security Researchers is online and up to date.

Annex B: Example Responsible Vulnerability Disclosure Policy

B1. Introduction

This policy aims to define a process by which security researchers can work with **[The Organisation]** to help improve the security of our products and services.

[The Organisation] takes security and the trust of our users very seriously. The responsible disclosure of security vulnerabilities helps us to ensure the security and privacy of our users. We are committed to thoroughly investigating and resolving security issues on our platforms and services.

B2. In Scope

<< This section should describe the type of service you authorise for external vulnerability assessment. >>

This disclosure policy applies only to vulnerabilities in **[The Organisation's]** products and services under the following conditions:

- Only domains/subdomains which have a security.txt file in their root (i.e. https://<subdomain.domain.tld>/security.txt[1]) are in scope. Currently, the scope is limited [http://organisationdomain]

B3. Out of scope

<< This section should describe the type of service that are not considered relevant for external vulnerability assessment as well as vulnerability submissions that are not considered for reward. The list below serves as an example>>

Any services hosted by 3rd party 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 test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Findings from applications or systems not listed in the 'Scope' section
- UI and UX bugs and spelling mistakes
- Reports of non-exploitable vulnerabilities and/or reports indicating that our services do not fully align with "best practice" (e.g. missing security headers) are not in scope.
- Network level Denial of Service (DoS/DDoS) vulnerabilities
- TLS configuration weaknesses (e.g. "weak" ciphersuite support, TLS1.0 support etc.) are not in scope.
- Volumetric vulnerabilities are not in scope (i.e. simply overwhelming our service with a high volume of requests is not in scope).

Things we do not want to receive:

- Personally, identifiable information (PII)
- Credit card holder data

[1] https://tools.ietf.org/html/draft-foudil-securitytxt-05

B4. Rewards

<< This section should describe the type of reward your company proposes for the category of vulnerabilities considered.>>

[Financial reward example]

We would like to offer a paid reward to security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy. The amount is available is set according to the criticality and relevance of the vulnerability. Reporters of qualifying vulnerabilities will be **paid according to the reward scale** here and special **acknowledgement of achievements** on the company's website.

[Non-Financial reward example]

Unfortunately, due to **[The organisation's]** funding structure, it is not currently possible for us to offer a paid bug bounty programme. We would, however, like to offer a token of our appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy. Reporters of qualifying vulnerabilities will be offered a unique **Company** reward and special **acknowledgement of achievements** on the company's website.

B5. Mandatory Rules

<< This section describes the rules and limitations within which the researcher can conduct his investigation on the media company's services and assets. >>

Responsible security researchers understand that the integrity and security of our customers is our priority and will work with **[The Organisation]** to ensure that all necessary vulnerabilities are resolved, and that customers have ample opportunity to deploy the fixes required before releasing information regarding their finding on a public forum, blog, or social media.

The [**company vulnerability disclosure e-mail] address** is only to be used for submitting potential product vulnerabilities. Regular product or service support should be directed to your authorized **[The Organisation]** Technical Support E-mail [(**company customer support disclosure e-mail**)].

Security researchers must not:

- Access unnecessary amounts of data. For example, 2 or 3 records is enough to demonstrate most vulnerabilities (such as an enumeration or direct object reference vulnerability);
- Violate the privacy of [**The Organisation]** users, staff, contractors, systems etc. For example, by sharing, redistributing and/or not properly securing 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 **[The Organisation]** security contact;
- Modify data in our systems/services which is not your own;
- Place or insert any kind of malicious code on the system;
- Disrupt our service(s) and/or systems; or
- Disclose any vulnerabilities in **[The Organisation]** systems/services to 3rd parties/the public prior to **[The Organisation]** confirming that those vulnerabilities have been mitigated or rectified. This does not prevent notification of a vulnerability to 3rd parties to whom the vulnerability is directly relevant, for example where the vulnerability being reported is in a software library or framework – but details of the specific vulnerability of **[The Organisation]** must not be referenced in such reports. If you are unsure about the status of a 3rd party to whom you wish to send notification, please e-mail [security@mediacompany.com] for clarification.
- **[The Organisation]** requests that all data retrieved during research is securely deleted as soon as it is no longer required and at most, ***XX*** month(s) after the vulnerability is resolved, whichever occurs sooner.

If you are unsure at any stage whether the actions you are thinking of taking are acceptable, please contact our security team for guidance (please do not include any sensitive information in the initial communications): [security@mediacompany.com].

B6. Reporting a vulnerability

<< This section describes how to submit a vulnerability and what should be included in the submission. >>

If you have discovered an issue which you believe is an in-scope security vulnerability (please see section above for more detail on scope), please e-mail **[security@mediacompany.com]** including:

- The website or page in which the vulnerability exists.
- A brief description of the class (e.g. "XSS vulnerability") of the vulnerability. **Please avoid including any details which would allow reproduction of the issue at this stage**. Detail will be requested subsequently, over encrypted communications.

In accordance with industry convention, we ask that reporters provide a benign (i.e. non-destructive) proof of exploitation wherever possible. This helps to ensure that the report can be triaged quickly and accurately whilst also reducing the likelihood of duplicate reports and/or malicious exploitation for some vulnerability classes (e.g. sub-domain takeovers).

Please ensure that you do not send your proof of exploit in the initial, plaintext email if the vulnerability is still exploitable. Please also ensure that all proof of exploits is in accordance with our guidance (below), if you are in any doubt, please e-mail **[security@mediacompany.com]** for advice.

Please read this document fully prior to reporting any vulnerabilities to ensure that you understand the policy and can act in compliance with it.

B7. What to expect

<< This section describes the management procedure for any vulnerability submission. >>

In response to your initial e-mail to **[security@mediacompany.com]** you will receive an acknowledgement e-mail from **[The Organisation]** Security Team, usually within **xx** hours of your report being received. The acknowledgment e-mail will include a ticket reference number that you can quote in any further communications with our Security Team.

Attached to the acknowledgement email will be a PGP key which you can use to encrypt future communications containing sensitive information. Following the initial contact, our Security Team will work to triage the reported vulnerability and will respond to you as soon as possible to confirm whether further information is required and/or whether the vulnerability qualifies as per the above scope or is a duplicate report.

From this point, necessary remediation work will be assigned to the appropriate **[The Organisation]** teams and/or supplier(s). Priority for bug fixes and/or mitigations will be assigned based on the severity of impact and complexity of exploitation. Vulnerability reports may take some time to triage and/or remediate; you are welcome to enquire on the status of the process but please limit this to no more than once every 14 days, this helps our Security team focus on the reports as much as possible. Our Security Team will notify you when the reported vulnerability is resolved (or remediation work is scheduled) and will ask you to confirm that the solution covers the vulnerability adequately.

We will offer you the opportunity to feed back to us on the process and relationship as well as the vulnerability resolution. This information will be used in strict confidence to help us improve the way in which we handle reports and/or develop services and resolve vulnerabilities. We will also offer to include reporters of qualifying vulnerabilities on our acknowledgments page and we'll ask for the details you wish to be included.

B8. Legal Framework

<< This section describes the laws and regulations under which the researcher must conduct his investigation. The listed laws usually match the country's legal regulation around cybercrime and data protection. >>

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 **[The Organisation]** to be in breach of any of its legal obligations, including but not limited to:

<< Replace the list of laws here with relevant laws from your own jurisdiction, the examples below are only relevant in Ireland. >>

- Data Protection Act 1988
- Criminal Damage Act 1991
- Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993
- Data Protection (Amendment) Act 2003
- Criminal Justice (Theft and Fraud Offences) Act 2001
- Criminal Justice Act 2011
- Criminal Justice (Offences Relating to Information Systems) Act 2017
- The General Data Protection Regulation 2016/679 (GDPR) and The Data Protection Act 2018.

[The Organisation] 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 **[The Organisation]** service.

B9. References

[1] *OWASP – Open Web Application Security Project* - "Vulnerability Disclosure Cheat Sheet". https://www.owasp.org/index.php/Vulnerability_Disclosure_Cheat_Sheet

[2] *BBC's Security Disclosure Policy https://www.bbc.com/backstage/security-disclosure-policy/*