Introduction

This policy aims to define a process by which security researchers can work with TV 2 Danmark A/S (TV 2) to help improve the security of our products and services. TV 2 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.

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

In Scope

This disclosure policy applies only to vulnerabilities in TV 2 products and services under the following conditions:

- Only domains/subdomains which have a security.txt file :
  (i.e. https://tv2.dk/.well-known/security.txt) are in scope.

Out of scope

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
- 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).
- Reports of non-exploitable vulnerabilities and/or reports indicating that our services do not fully align with "best practice" e.g. missing security headers (CSP, x-frame-options, x-prevent-xss etc) or suboptimal email related configuration (SPF, DMARC etc) are not in scope.

Bug Bounties

TV 2 does not have a bug bounty/reward program and will therefore not offer paid bug rewards. We do offer tokens of our appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities to us.

Reporting a vulnerability

If you have discovered an issue which you believe is an in-scope security vulnerability (please see section 2 above for more detail on scope), please user the details in security.txt or email itsecurity@tv2.dk 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.

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 proofs of exploits are in accordance with our guidance (below), if you are in any doubt, please email itsecurity@tv2.dk for advice.

Mandatory rules / Guidelines

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 TV 2 users, staff, contractors, customers, 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 TV 2 security contact
- Modify data in our systems/services which is not your own
- Disrupt our service(s) and/or systems; or
- Disclose any vulnerabilities in TV 2 systems/services to 3rd parties/the public prior to the TV 2 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 TV 2 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 email itsecurity@tv2.dk for clarification.

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.

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): itsecurity@tv2.dk.

What to expect

in response to your initial email to itsecurity@tv2.dk you will receive an acknowledgement reply email from the TV 2 Security Team, this is usually within 24 hours of your report being received. The acknowledgment email will include a ticket reference number which 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 TV 2 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're welcome to enquire on the status of the process.

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 in order 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.

Legalities

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 any law or cause the TV 2 to be in breach of any of its legal obligations