WMDA Vulnerability Disclosure Policy

- Introduction
- Systems in Scope
- Out of Scope
- Our Commitments
- Our Expectations
- Official Channels
- Technical guidelines
- Safe Harbour

Introduction

WMDA welcomes feedback from security researchers and the general public to help improve our security.

If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you.

This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

Systems in Scope

This policy applies to any digital assets owned, operated, or maintained by WMDA. This includes (but is not limited to) any system available via *.wmda.info, *.wmdd.org, *.worldmarrowdonorday.org

Out of Scope

Assets or other equipment not owned by parties participating in this policy. Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or applicable authority.

Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbour for your vulnerability research that is related to this policy.

Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;
- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept;
- and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Official Channels

Please report security issues via email to security@wmda.info , providing all relevant information. The more details you provide, the easier it will be for us to triage and fix the issue.

Technical guidelines

You should encrypt any confidential information with GPG using key E557DAF22D9608C3 : E233AE50095899214A41366DE557DAF22D9608C3.asc

The public key is also available at https://keyserver.ubuntu.com/pks/lookup?op=get&search=0xe233ae50095899214a41366de557daf22d9608c3

Security information and fingerprints are also available in the _security.* TXT records in the DNS of wmda.info. (online)

The link to the current policy will be available following the security.txt recommendations

Safe Harbour

When conducting vulnerability research, according to this policy, we consider this research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy;
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms of Service (TOS) and/or Acceptable Usage Policy (AUP) that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws.

If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Note that the Safe Harbour applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

This policy has been compiled with help of the templates of disclose.io