MX Public Vulnerability Disclosure Policy

Purpose

MX is committed to ensuring the safety and security of our customers. Towards this end, MX is now formalizing our policy for accepting vulnerability reports in our products. We hope to foster an open partnership with the security community, and recognize that the work the community does is important in continuing to ensure safety and security for all of our customers. We have developed this policy to both reflect our corporate values and to uphold our legal responsibility to good-faith security researchers that are providing us with their expertise.

Initial Scope

MX's Vulnerability Disclosure Program initially covers the following products

- Atrium (atrium.mx.com)

Response

MX will make a best effort to quickly respond to and resolve responsibly disclosed issues.

Rewards

At this time, MX does not offer a monetary reward for the responsible disclosure of security vulnerabilities. Security researchers who report qualifying issues will receive public acknowledgement in our release notes. If you would like to keep your report confidential, please indicate in your communication with us that you prefer not to receive public acknowledgement.

Program Rules

Only test assets that are in scope.

Please provide detailed reports with reproducible steps.

Submit one vulnerability per report.

Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.

The following activity and methods are prohibited:

- Social engineering of any kind
- Spamming
- Denial of service
- Reverse Engineering
- Physical attacks against MX property or data centers

How to Submit a Vulnerability

To submit a vulnerability report to MX's Security Team, please email vulns@mx.com and use our public key for all communications

Report Acceptance Criteria

We will use the following criteria to decide whether or not to accept the report. Reports that are out of scope, proven to be a false positive, not of sufficient quality or did not provide enough detail to be actionable will be declined or rejected. We will make a best effort to provide this feedback to the researcher and provide evidence where possible..

What we would like to see from you:

- Well written reports in English will have a higher chance of being accepted.
- Reports that include proof of concept code will be more likely to be accepted.
- Reports that include only crash dumps or other automated tool output will most likely not be accepted.
- Include how you found the bug, the impact, and any potential remediation.
- Consideration for vulnerabilities that may have safety impact.
- Any plans for public disclosure.

What you can expect from us:

- A timely response to your email (within 3 business days; if you don't receive a response in that time, please reach out again).
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- An expected timeline for patches and fixes (usually within 120 days).
- Credit after the vulnerability has been validated and fixed.