CSX Responsible Disclosure Policy

CSX understands that protection of customer data is a significant responsibility and requires our highest priority. We therefore take the security of our systems extremely seriously, and we genuinely value the assistance of security researchers and others in the security community to assist in keeping our systems secure. The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of all our users.

- ✓ Key guiding principles of our responsible disclosure policy include:
- ✓ Ensuring that the vulnerability is not publicly disclosed before CSX has had a reasonable period of time to fix the vulnerability; and
- ✓ Keeping communication channels open to allow effective collaboration.

Scope

This program is limited to exploitable security vulnerabilities in [CSX systems and websites]. Services hosted by third party providers are excluded from this program and the scope of the policy. Vulnerabilities found in non-CSX systems should be reported directly to the third party provider.

Guidelines For Responsible Disclosure

We require that all researchers:

- ✓ Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- ✓ Perform research only within the scope set out in this policy;
- ✓ Use the identified communication channels to report vulnerability information to us; and
- ✓ Keep information about any vulnerability you've discovered confidential between yourself and CSX until we've had 45 days to resolve the issue [a reasonable amount of time to resolve the issue].
- ✓ Engage in testing of systems and research without harming CSX or its customers, attempting to access our offices, data centers or user accounts, violating any applicable laws, disrupting or compromising data or further exploiting a confirmed vulnerability.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets), you must stop your test, notify us immediately and not disclose the data to anyone else.

If you comply with our responsible disclosure policy when researching and reporting an issue to us, we commit to:

- ✓ Not pursue or support any legal action against you related to your research;
- ✓ Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission); and
- ✓ Maintain a good collaborative relationship with you and recognize your contribution on our Security Researcher Hall of Fame, if you are the first to report the issue and we make a code or configuration change based on the issue.

Qualifying Security Bugs

What is a qualifying vulnerability?

Injection vulnerabilities such as XSS, XXE, CSRF, SQLi, Local or Remote File Inclusion, authentication issues, buffer overflows, timing attacks, remote code execution, and authorization issues, privilege escalation and clickjacking. You must be the first researcher to responsibly disclose the vulnerability and you must follow the responsible disclosure principles set out in this policy, which include giving us a reasonable amount of time to address the vulnerability.
The reasonable amount of time will be discussed with you and determined following the disclosure of the vulnerability.

What is not a qualifying vulnerability?

Each submission will be evaluated on a case-by-case basis. Below is a list of some of the issues which don't qualify as security vulnerabilities:

- UI and UX bugs and spelling mistakes;
- TLS/SSL related issues;
- SPF, DMARC, DKIM configurations;
- Vulnerabilities due to out of date browsers or plugins;
- Content-Security Policies (CSP);
- Vulnerabilities in end of life products;
- Lack of secure flag on cookies;
- Username enumeration;
- Vulnerabilities relying on the existence of plugins such as Flash;
- Security headers missing such as, but not limited to "content-type-options", "X-XSS-Protection";
- CAPTCHAs missing as a Security protection mechanism;
- Issues that involve a malicious installed application on the device;
- Vulnerabilities requiring a jailbroken device;
- Vulnerabilities requiring a physical access to mobile devices;
- Use of a known-vulnerable library without proof of exploitability;
- Tap-jacking and UI-redressing attacks that involve tricking the user into tapping a UI element;
- Distributed Denial of Service (DDOS) attacks;
- Lack of rate limiting, brute force attacks;
- Lack of a session timeout;
- CSV injection;
- Self-XSS;
- Directory listing;
- Best practices concerns;
- Banner grabbing (such as finding the version of a service);
- Vulnerabilities in only one browser; and
- Theoretical issues reported by popular scanners that have not been validated and [to?] provide demonstrable impact.

Report A Security Vulnerability

If you believe you've found a security vulnerability in one of our products or platforms please report it by emailing our security team. Please include the following details with your report:

- ✓ Description of the location and potential impact of the vulnerability;
- ✓ A detailed description of the steps required to reproduce the vulnerability; and
- ✓ Your name/handle and a link if you would like to be included on our Security Researcher Hall of Fame for recognition.

CSX does not participate in a bug bounty awards program at this time. However, when a qualifying vulnerability is confirmed and remediated, we will offer to recognize and credit the security researcher on our Security Researcher Hall of Fame. If you prefer not to be recognized, reports may be submitted anonymously.

Legal Notice: By submitting a report to CSX, you warrant that the report and any attachments do not violate the intellectual property rights of any third party and grant to CSX a non-exclusive, royalty-free, world-wide, perpetual license to use, reproduce, create derivative works, and publish the report and any attachments.

Security Research Wall Of Fame

CSX would like to publicly convey our deepest gratitude to the following security researchers for responsibly disclosing vulnerabilities and working with us to remediate them.
Your legendary efforts are truly appreciated by CSX.

2020