CSBS Vulnerability Disclosure Policy

Approved 09/17/2005

The Conference of State Bank Supervisors (CSBS) is committed to protecting the confidentiality, integrity, and availability of the systems and data entrusted to us by state regulators, supervised institutions, and the public. We welcome good-faith reports of potential vulnerabilities in our systems so that we can investigate and remediate them.

Please note: CSBS does not offer financial rewards or operate a bug bounty program. This policy exists solely to provide a clear and safe process for reporting vulnerabilities to our security team.

Scope

This policy applies only to CSBS-owned or operated systems and digital services expressly identified as in-scope below and on our public website. Any services not expressly listed below, such as any connected services, are excluded from scope and are not authorized for testing.

- **In Scope:**
  - *.csbs.org
  - *.nmls.org
  - *.statemortgageregistry.com
  - *.nmlsconsumeraccess.org
  - *.nationwidelicensingsystem.org
  - *.stateexaminationsystem.org
  - *.stateregulatoryregistry.org

- **Out of Scope:**
  - Third-party services or platforms not managed by CSBS (report issues directly to the provider/platform owner).
  - Physical testing (e.g., office access, badge cloning, tailgating).
  - Social engineering (e.g., phishing, vishing, pretexting).
  - Denial-of-service (DoS/DDoS) or resource-exhaustion attacks.
  - Automated scanning or brute force testing.
  - User interface bugs, typos, or other non-security issues.

If you are uncertain whether a system is in scope, contact us before beginning any research.

Guidelines for Researchers

When conducting security research under this policy, you must:

1. Act in good faith to avoid actions that could harm CSBS, our member agencies, or the financial institutions we support.
2. Respect privacy: Do not intentionally access, copy, modify, or delete data. If you encounter sensitive data (such as personally identifiable information (PII) or financial records), stop immediately, purge the data, and report the finding.
3. Limit exploitation: Use proof-of-concept exploits only to the extent necessary to confirm a vulnerability. Do not attempt to establish persistence, exfiltrate data, or pivot to other systems.
4. Do no harm: Do not disrupt services, degrade system performance, or initiate fraudulent financial transactions.
5. Allow remediation time: Give CSBS a reasonable amount of time to validate and remediate the issue before disclosing publicly.

Safe Harbor

If CSBS determines that you followed this policy and conducted security research in good faith:

- CSBS will not pursue legal action against you.
- CSBS will communicate, where appropriate and legally permissible, that your research was conducted under this policy.

Activities outside the scope of this policy or that violate applicable laws are not authorized and may result in legal action.

Reporting a Vulnerability

To report a potential vulnerability:

- Email: security@csbs.org
- Include:
    - A description of the vulnerability and its potential impact.
    - Steps to reproduce (including tools or scripts used).
    - Screenshots or proof-of-concept code, clearly labeled.
    - Your contact information (if you wish to be acknowledged).

Please do not include sensitive data (PII, financial information) in your report. If such data must be shared to validate an issue, indicate this in your report, and we will establish a secure channel.

Our Commitment

CSBS will:

- Acknowledge receipt of reports within 5 business days.
- To the best of our ability and as deemed appropriate, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to security@csbs.org. We also invite you to contact us with suggestions for improving this policy.