RESPONSIBLE DISCLOSURE POLICY

Introduction

The California State Lottery (the Lottery) is committed to ensuring the security and integrity of its games. This policy is intended to provide security researchers with clear guidelines for conducting vulnerability discovery activities and to convey the Lottery's preferences for communicating discovered vulnerabilities.

This policy describes which systems and research types are covered, how to submit vulnerability reports, and how long the Lottery asks security researchers to wait before publicly disclosing vulnerabilities.

The Lottery encourages you to contact us at ResponsibleDisclosureIntake@CALottery.com to report potential vulnerabilities in its systems.

Authorization

If you make a good-faith effort to comply with this policy during your cybersecurity research, the Lottery will consider your research to be authorized. The Lottery will work with you to understand and resolve the issue quickly, and it will not recommend or pursue legal action related to your research. Should legal action be initiated against you by a third party for activities conducted in accordance with this policy, the Lottery will make this authorization known upon inquiry or request.

Guidelines

Under this policy, "research" means activities in which you:

- Notify the Lottery as soon as possible after you discover a real or potential cybersecurity issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Do not use an exploit to compromise or exfiltrate the Lottery's data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide a reasonable amount of time for the Lottery to resolve the issue before you disclose it publicly.

Once you have established that a vulnerability exists or encounter any sensitive or confidential data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify the Lottery immediately, and not disclose this data to anyone else. Failure to do so may result in legal action by the Lottery.

Scope

This policy applies to the following Lottery systems and services:

- CALottery.com
- California Lottery Official App (mobile device application)

Any services not expressly listed above, such as any connected services, are excluded from the scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside this policy's scope and should be reported directly to the vendor, per their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at ResponsibleDisclosureIntake@CALottery.com before starting your research.

Although the Lottery develops and maintains other internet-accessible systems or services, we request that active research and testing be conducted only on the systems and services covered by the scope of this policy. If there is a particular system not in scope that you believe merits testing, please get in touch with ResponsibleDisclosureIntake@CALottery.com to discuss it first. The Lottery reserves the right to update the scope of this policy over time.

Test Methods
The Lottery does not authorize the following test methods:
- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data;
- Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.

Reporting a Vulnerability
The Lottery accepts vulnerability reports via ResponsibleDisclosureIntake@CALottery.com. Reports may be submitted anonymously. If you share contact information, the Lottery will acknowledge receipt of your report within 10 business days. By submitting a vulnerability report, you acknowledge that you have no expectation of payment and that you expressly waive any present and future compensation claims against the Lottery related to your submission.

What the Lottery would like to see from you
To assist the Lottery with triaging and prioritizing submissions, it is recommended that your reports:
- Describe in English the location where the vulnerability was discovered and the potential impact of exploitation;
- Offer a detailed description of the steps needed to reproduce the vulnerability. (Proof of concept scripts, code used to exploit, and screenshots are helpful.)

What you can expect from the Lottery
- When you choose to share your contact information with the Lottery, we commit to coordinating with you as openly and as quickly as possible.
- Within 10 business days, the Lottery will acknowledge that your report has been received.
- To the extent practicable and appropriate, the Lottery will maintain an open dialogue with you to discuss issues.

Questions
Questions regarding this policy may be sent to ResponsibleDisclosureIntake@CALottery.com.