Introduction

Cryptosmartlife recognizes the importance and value of security researchers' efforts in helping keep our platform safe. We encourage responsible disclosure of security vulnerabilities via our bug bounty program ("Bug Bounty Program") described on this page.

Note: This program is for the disclosure of software security vulnerabilities only. If you believe your Cryptosmartlife account has been compromised, change your password and immediately contact support via our [support email]

The Bug Bounty Program scope covers all software vulnerabilities in services provided by Cryptosmartlife.

A valid report is any in-scope report that clearly demonstrates a software vulnerability that harms Cryptosmartlife or Cryptosmartlife customers. A report must be a valid, in scope report in order to qualify for a bounty. Cryptosmartlife will determine in its sole discretion whether a report is eligible for a reward and the amount of the award.

Program Policies

Researcher Requirements

Complying with the Bug Bounty Program policy requires researchers to adhere to "Responsible Disclosure". Responsible Disclosure includes:

1. Providing Cryptosmartlife a reasonable amount of time to fix a vulnerability prior to sharing details of the vulnerability with any other party.
2. Making a good faith effort to preserve the confidentiality and integrity of any Cryptosmartlife customer data.
3. Not defrauding Cryptosmartlife customers or Cryptosmartlife itself in the process of participating in the Bug Bounty Program.
4. Not profiting from or allowing any other party to profit from a vulnerability outside of Bug Bounty Program payouts from Cryptosmartlife.
5. Reporting vulnerabilities with no conditions, demands, or ransom threats.

Cryptosmartlife considers Social Engineering attacks against Cryptosmartlife employees to be a violation of Program Policies. Researchers engaging in Social

Engineering attacks against Cryptosmartlife employees will be banned from the Cryptosmartlife Bug Bounty program. We define Social Engineering as acts that influence people to perform security-impacting actions or divulge confidential information.

Report Evaluation

Cryptosmartlife Security
In order to be deemed valid, a report must demonstrate a software vulnerability in a service provided by Cryptosmartlife that harms Cryptosmartlife or Cryptosmartlife customers. Reports that include a clear Proof of Concept or specific step by step instructions to replicate the vulnerability are considerably more effective at communicating a researcher's findings and are therefore far more likely to be deemed valid.

A report must be a valid, in scope report in order to qualify for a bounty. Cryptosmartlife awards bounties based on severity of the vulnerability. We determine severity based on two factors: Impact and Exploitability.

Impact describes the effects of successful exploitation upon Cryptosmartlife systems or customers. We make this assessment primarily by examining the effects of exploitation on confidentiality, integrity, or availability of underlying information. Vulnerabilities that require considerable response and remediation efforts or could result in reputational damage are also considered to have greater impact. For example:

- Critical Impact: Attackers can read or modify Sensitive Data in a system, execute arbitrary code on the system, or exfiltrate digital or fiat currency in some way.
- Low Impact: Attackers can gain small amounts of unauthorized, low sensitivity information impacting a subset of users, or slightly impact accuracy and performance of a system. (Please note that Denial of Service bugs will be considered on a case-by-case basis. Denial of Service issues that don't impact availability of funds or user data will not likely be accepted as a valid report.) Lack of rate limiting in Cryptosmartlife products will be not considered valid unless a critical impact to the environment is demonstrated

Exploitability describes the difficulty of actively exploiting the vulnerability itself. We make this assessment primarily based on the prerequisites for exploitation, including level of access required, availability of information critical for successful exploitation,

and likelihood of alignment of required factors outside the attacker's direct control such as social engineering requirements or timing requirements. For example:

- Critical Exploitability: Attackers can unilaterally exploit the finding without significant roadblocks or special conditions outside attacker control.
- Low Exploitability: Exploitation is difficult due to several requirements, such as access limitations, complicated social engineering, guessing unknown values, or alignment of unpredictable race conditions.

Severity is determined as a combination of Impact and Exploitability. For example:

- Critical Severity: a state of immediate, easily accessible threat of large-scale compromise or irreversible damage to Cryptosmartlife or Cryptosmartlife customers.
- Low Severity: a state of no immediate threat where an opportunity exists for an improvement that may mitigate a potential future vulnerability.

In order to provide general guidelines to researchers regarding the payouts that can be expected for a given report, Cryptosmartlife uses the severity of a report to place the report into one of the following tiers.

Vulnerability Tier	**Reward**
Critical	$xxx
High	$xxx
Medium	$xxx
Low	$xx

The payouts listed next to each tier are minimum bounties for the tier. Bonuses in excess of the tier minimum can be awarded based on the severity of the vulnerability or creativity of the exploitation. Researchers are also more likely to earn a larger reward for exceptionally clear and high-quality reports.

Previous bounty amounts are not considered precedent for future bounty amounts. Software is constantly changing and therefore the given security impact of the exact same vulnerability at different times in the development timeline can have drastically different security impacts.

Report Closure

Cryptosmartlife reviews all findings that are reported via our Bug Bounty Program. Each report submission is reviewed and evaluated to ensure validity. If the description in the report is unclear, Cryptosmartlife will request additional information from the reporter. After all information is aggregated; the report submission goes through an internal review and scoring process. After the internal review process is complete, any bugs that are not reproducible, invalid or informative will be closed.

PLEASE NOTE: It is up to the researcher to provide detailed information and supporting evidence to support all reports. Failure to provide a detailed report will result in delayed triage and/or ticket closure.

Scope

The Cryptosmartlife Bug Bounty program scope covers all software vulnerabilities in services provided by Cryptosmartlife.

Specific domains hosting Cryptosmartlife services are provided below:

- *.cryptosmartlife.com (All assets on cryptosmartlife.com and subdomains, excepting services provided by third parties)
- com.cryptosmartlife.android (Android: Play Store Cryptosmartlife app)
- com.cryptosmartlife.ios (iOS: App Store Cryptosmartlife app)

Please view the scope section for a more detailed list of in-scope and out-of-scope assets.

Additionally, all vulnerabilities that require or are related to the following are out of scope:

- Social engineering
- Rate Limiting (Non-critical issues)
- Physical security
- Non-security-impacting UX issues
- Deprecated Open Source libraries are not in scope.

- Vulnerabilities or weaknesses in third party applications that integrate with Cryptosmartlife
- Ability to abuse existing banking functionality such as ACH or credit card chargebacks

If you feel that a particular asset or activity not mentioned here should be in scope, please submit a report along with a brief description of why you believe that the asset should be covered by this scope.