AarogyaSetu Bug Bounty Programme

(for Android App)

Contents

1. Background

AarogyaSetu is a mobile application developed by the Government of India to protect the citizens of India in our combined fight against COVID-19. The App is aimed at augmenting the initiatives of the Government of India in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19. Developers of AarogyaSetu take security issues very seriously and recognize the importance of privacy, security, and community outreach.

Government is committed to keep AarogyaSetu application, its supporting systems, data and network secure and address any security issues through a coordinated and constructive approach designed to drive the best possible protection for our citizen data.

AarogyaSetu application is developed keeping in mind the "Privacy by design principle". Despite the best measures taken, the presence of vulnerabilities may exist. When such vulnerabilities are found, Government would like to learn of them as soon as possible, allowing it to take swift action to fix them and thereby enhance the security. In addition to security, suggestions for code change for enhanced efficiency are also encouraged.

AarogyaSetu's **Bug Bounty Programme** has been prepared with thegoal to partner with security researchers and Indian developer community to test the security effectiveness of AargoyaSetu and also to improve or enhance its security and build user's trust.

2. How the Programmewill work

2.1.1 AarogyaSetu production build of the androidapp, followed by the iOS along with API documentation will be made available to open source research community.

2.1.2 Everyone, including researchers and Users of AarogyaSetu, are encouraged to report any vulnerability impacting the privacy and information security posture of AarogyaSetu application.

2.1.3 Security or Privacy related flaws discovered by the security researchers should be notified to : as-bugbounty@nic.in only, with subject line : Security Vulnerability Report, so that Aarogya Setuteam can first verify the vulnerability (if any) and take action to fix the vulnerability . Doing so will be called `**responsible disclosure'** and only such responsible disclosures shall be eligible for rewards.

2.1.4 Any improvements to the source code of AarogyaSetu can also be reported to as-bugbounty@nic.in, with the subject line : Code Improvement

2.1.5 Security Researchers will document their findings thoroughly, providing steps to reproduce and send report to us at as-bugbounty@nic.in. Reports with complete vulnerability details, including screenshots or video of POC, are essential for being eligible for reward.

2.1.6 AarogyaSetu Team will contact the researchers to confirm that we've received the report and trace steps to reproduce the research.

2.1.7 AarogyaSetu Team will notify researcher of remediation and may reach out for questions or clarification.

2.1.8 AarogyaSetu Team will work to make necessary improvements and remediation to fix the vulnerability.

2.1.9 Only those submissions that meet the following eligibility requirements and the Rules mentioned in Section 5.0, may receive a reward:

- The vulnerability must be a qualifying vulnerability (see Scope)
- Security Researcher may not publicly disclose the vulnerability prior to our resolution.
- The Researcher/Company reporting the vulnerability/code improvements should not be employed/working for AarogyaSetu Project or its related activities/initiatives.
- Employees (including their family members) of National Informatics Centre (NIC) and Ministry of Electronics & IT (MeitY) and its constituent organizations are not eligible.

3. Scope

3.1 The in-scope application will be:

The production build of theAarogyaSetuAndroid application

3.2 In-Scope Vulnerabilities

The following vulnerabilities shall be eligible for a reward, provided that these vulnerabilities should be exploitable on an unrooted phone running a version of Android supported by Aarogya Setu, with ADB Disabled and with all default android security features in place:

1) By exploiting the vulnerability, one should be able to access an individual's Aarogya Setu data on an Androidphone, or remotely submit a self-assessment through the phone.

2) By exploiting the vulnerability, one should be able to access other people's data from an individual's app or phone - other than their own AarogyaSetu data and other than Digital ID (DiD) data broadcast by bluetooth in the vicinity of the phone

3) The Vulnerability should be able to Compromise Aarogya Setu servers or hack the servers such that the servers become buggy, crash or expose any personal data other than the User's own data or services already provided by the existing APIs

Please note that the reported vulnerability should be present in the AarogyaSetu App or its source code or back end Server. Any vulnerabilities or exploits which are related to the platform (i.e., Operating System, Cloud, Web Server, Database…etc) and technology/services (like Bluetooth, GPS, SMS...etc), shall not be considered for the bug bounty reward.

3.3 In-Scope Code Improvements

The suggested code improvement should have a significant impact on the App's overall performance improvement, battery usage reduction, memory and bandwidth reduction. There should be a minimum of 10% or more performance impact over and above the existing performance of the App on all supported android versions. The submission for the code improvement should contain, the

detailed programme code change, test data and a Proof of Concept, demonstrating the impact of the code change. By implementing the code improvement, there should not be any degradation across all supported android versions and it should not lead to any security vulnerabilities or issues.

4. Vulnerability and Code ImprovementsRating and Rewards

The exploitability of the reported Vulnerabilities should be viewed in the context of a normal smartphone user. The ease of exploitability, the impact of the vulnerability and amount/type of personal data (of other Users) exposed. Shall be factored in while shortlisting the reported vulnerability to be considered for a reward.

Security Researcher will qualify for a reward if he/she is the first person to alert the AarogyaSetuTeam to a previously unknown valid security vulnerability and if the reported vulnerabilityconfirms to the Scope mentioned in Section 3.0.

In addition to providing rewards for responsible disclosure of the vulnerability, appropriate rewards shall be awarded to the Researchers who makes responsible disclosure for anysuggestions onthe improvements in the source code or the Application from a security perspective. While providing the suggestions the Researchers should provide the detailed code snippet for implementing their suggestion/improvement. They should also ensure that upon implementing their suggestion/improvement, the App should still work on all supported devices (i.e., Android version 5.0 and above), with all existing functionalities and features intact.

RewardCategories

Bounty /Reward Category	***Maximum Reward Amount (in INR)***	***Email ID for reporting***
Security Vulnerability	*Rs.300000 (Rupees Three Lakhs)* *Upto Rs.100000 (Rs One lakh) per vulnerability mentioned under point 3.2 "in-scope vulnerabilities". Submission can be done for one individually or all three. Please mention in the submission accordingly.*	*As-bugbounty@nic.in*

Suggestion / Improvement in the Source code	*Upto Rs.100000 (Rupees One Lakh) for the in-scope code improvements mentioned under point 3.3*	*As-bugbounty@nic.in*

- All submissions that qualify as per the terms of this notification shall receive a certificate of appreciation.
- If more than one qualifying submission is received from multiple researchers/companies, then the Aarogya Setu team may shortlist the submissions based on their ease of exploitation, severity, impact and exposure of data (if any), for further consideration. The reward amount may be divided accordingly.

5. Rules for reporting a Vulnerability or a Code improvement

- This Bug bounty programme is open to people residing in India.
- People residing outside India may also make submissions in the bug bounty but they shall not be eligible for any rewards. However, if they make any valid submissions which are shortlisted by the Aarogya Setu team, they would be issued a certificate of appreciation for their contribution.
- This Bug bounty programme is open from **00:00 hrs 27-May-2020 to 23:59 hrs 26-June-2020**. Only entries received between this period shall be considered for the reward.
- If a disclosed vulnerability or source code improvement is shortlisted for the reward, then the researcher shall provide his/her Government ID Proof, bank account details...etc., in order to claim the reward amount.
- The submissions can be done either as an Individual or as a Group of Individuals (not more than 5) or in the name of an Organization. At the time of submission, this detail should be clearly mentioned. The person who is making a submission on behalf an Organization, should obtain due authorization from their respective Organization before making the submission and attach the authorization letter/mail as part of the submission.
- Security Researchers should not access any personal information that is not their own, including by exploiting any vulnerability that they may come across.

- In order to be considered for a reward, the submissions must be made exclusively to specified email ID :as-bugbounty@nic.in for both security vulnerabilities and code improvement. The submission should contain the name, address, company details if any and mobile number for further communication. The email address used for the submission will be used for all communications post submission. Communication received from any other email address will not be accepted. Use of anonymous email service or disposable email addresses for the submissions are not allowed.
- Actions which affect the integrity or availability of AarogyaSetu application are strictly prohibited.
- If the security researchernotices performance degradation on the target systems, they must immediately suspend their testing.
- Submissions may be closed if a Researcher is non-responsive to requests for information after 3 days.
- The Security Researcher should co-ordinate with the AarogyaSetu team in testing the effectiveness of the vulnerability mitigation.
- If the Security Researcher has come across or gained access to the personal data of other Users of AarogyaSetu, then He/She shall immediately stop the testing and inform AarogyaSetu team about the vulnerability.
- At no point of time, a Security Researcher shallcopy, save, disclose, retainor transfer the data or personal information of any User (apart from his/her own data) of the AarogyaSetu.
- Researchers while reporting the vulnerability should include a video or screenshot along with a Proof-of-Concept and a step wise instructionto demonstrate the vulnerability and its exploitation, in their submissions. These files should not be shared publicly. This includes uploading to any publicly accessible websites (i.e. YouTube, twitter, facebook, etc.).
- The Researcher should share detailed code snippet for the code improvements which are being proposed. The adverse security impact of not implementing the code improvement suggested by the Researcher, should also be provided in detail, along with necessary screenshots, evidences, Proof of Concepts (where applicable).
- Social engineering (e.g. phishing, vishing, smishing) is prohibited.
- Researchers shall take necessary precautions to avoid privacy violations, destruction of data, and interruption or degradation of AarogyaSetu service.
- Researchers should not perform DoS or DDoS attacks.
- Researchers should not run any automated or manual scans against the back-end infrastructure.

- The Vulnerability reported or the Source code improvement reported, should be original and should not be previously reported by anyone.
- The Researcher should be ready to work and co-ordinate with AarogyaSetu team in implementing the code improvement or bug fixes, testing the Application or code, debugging or troubleshooting issues related to the bug or code improvement.
- Code submitted as part of the submission should be the original work of the individual and all rights related to the code will be under the ownership of NIC.
- All communications made with the Aarogya Setu team with respect to the bug bounty programme should be kept confidential and should not be shared with anyone, nor posted on any public platforms. Doing so will disqualify the submission.
- At any point of time, if the information submitted by the researchers or companies is found to be false, then their submission shall be summarily rejected and they shall forfeit all rewards.
- The decision of Aarogya Setu team is final and binding on all aspects related to this bug bounty programme.
