Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
National Cybersecurity Centre NCSC

Q&A - Federal bug bounty programme

Version: 23.12.2022

Contents

1 What is a bug bounty programme?

The purpose of bug bounty programmes is to identify, document and fix any vulnerabilities in IT systems and applications in collaboration with ethical hackers. Ethical hackers use their own methods which allow them to identify vulnerabilities that cannot always be detected using conventional penetration tests or security reviews.

2 Why does the Federal Administration use bug bounty programmes?

Bug bounty programmes are an important source of support, allowing companies – and the Federal Administration – to proactively have their IT systems checked for vulnerabilities. It is an efficient method with a high return on investment (ROI) and improves public trust in the tested systems. Bug bounty programmes are based on crowdsourcing, i.e. they use the know-how of the security community.

The Federal Administration has an important role in setting an example for businesses and society. By institutionalising bug bounty, ethical hacking and crowdsourcing, the Federal Council is sending important signals with regard to boosting the cyber-resilience of the Swiss infrastructure.

3 What is the NCSC's role in the bug bounty programme?

The NCSC is responsible for the Federal Administration's bug bounty programme, and especially for procuring and managing the centralised platform used to run bug bounty programmes. In the bug bounty programmes themselves, the NCSC plays a coordinating and supporting role for the administrative units. It also reports regularly on the results of the Federal Administration's bug bounty programmes.

Specifically, it has the following tasks:

- Planning, prioritisation and implementation of programmes;
- Support to the administrative units in programme design and platform training;
- Coordination and communication between the administrative units and the platform operator, Bug Bounty Switzerland AG;
- Management and administration of the centralised bug bounty platform;
- Technical evaluation and triage of vulnerabilities in collaboration with Bug Bounty Switzerland;
- Communication in collaboration with the administrative units;
- Ensuring the compliance of the programmes' invoicing and payment procedures.

4 Why is the Federal Administration collaborating with Bug Bounty Switzerland AG?

The NCSC procured a centralised platform for bug bounty programmes in August 2022, and it will run future bug bounty programmes in the Federal Administration jointly with Bug Bounty Switzerland AG. Thanks to the established bug bounty platform and Bug Bounty Switzerland AG's large community of ethical hackers, the Federal Administration has the necessary tools

to successfully launch other bug bounty programmes. Bug Bounty Switzerland AG is one of the pioneers on the Swiss bug bounty scene. It has considerable expertise in running bug bounty programmes and collaborating with ethical hackers.

5 What is an ethical hacker in the bug bounty programme?

Ethical hackers are security experts who are contracted to check IT systems and products. They search for vulnerabilities that a malicious hacker might also be able to exploit. When searching for vulnerabilities, ethical hackers work within predefined guidelines set by the bug bounty programme. If they find a vulnerability, they report it and do not exploit it for personal gain. A reward is paid for any vulnerability found. The amount of the reward is based on the criticality of the vulnerability.

6 Which IT systems are checked?

The relevant Federal Administration units, in consultation with the NCSC, specify which systems are to be checked.

7 How high are the rewards (bounties)? Are they generally a fixed amount?

The bug bounty varies according to the criticality and relevance of the vulnerability. The bounties are set by the administrative units running the bug bounty programme, in consultation with the NCSC. As a result, they can vary from programme to programme. To ensure transparency, the possible bug bounty payments are fixed using a "bounty grid" at the start of the programme, and this is then communicated to the ethical hackers.

8 If vulnerabilities are discovered, does that mean that the Confederation has not done its job properly and that it is using an unsecured system? Why were the reported vulnerabilities not found earlier?

The pace of technological change is very rapid and new attack opportunities are opening up all the time. So IT security is an ongoing process. The purpose of bug bounty programmes is to identify, document and fix any vulnerabilities in IT systems and applications in collaboration with ethical hackers. Ethical hackers use their own methods which allow them to identify additional vulnerabilities that cannot always be detected using conventional penetration tests.

9 Isn't it irresponsible to let hacker loose on such important systems?

The hackers we employ are ethical hackers who are highly specialised and act very responsibly to search for vulnerabilities. Their aim is to use their activities for good and to help to continuously improve the tested systems' security. When taking part in a bug bounty programme, all ethical hackers must accept the programme guidelines and undertake to follow the set rules.

10 Why do you not publish the vulnerability reports in full?

For security reasons, no details of vulnerabilities are published. However, we do publish a summary of the results.

11 Are all the discovered vulnerabilities fixed immediately? What happens if a bug is discovered?

Each vulnerability is always analysed immediately and the risks are assessed. So the process of fixing the vulnerability depends on the risk of it being exploited and the potential damage that could ensue. Fixes for vulnerabilities are prioritised according to the risk assessment.

12 What criteria are used to select the ethical hackers?

The NCSC, which is responsible for the Federal Administration bug bounty programme, selects the ethical hackers together with Bug Bounty Switzerland AG. Selection is based on the programme scope and the technologies concerned. The focus is on the hackers' specialist knowledge, their availability and positive feedback from other bug bounty programmes.

Each ethical hacker is first vetted by Bug Bounty Switzerland AG ("know your customer" process).
In order to ensure that only identified and vetted ethical hackers can take part in the programmes – and that no transactions are performed with ethical hackers that are on a sanctions list, for example – Bug Bounty Switzerland AG checks the hackers' identity and integrity.
When taking part in a bug bounty programme, all ethical hackers must accept the programme guidelines and undertake to follow the set rules.
In most cases, the systems checked are publicly accessible online and do not require additional rights. These systems are generally already accessible to the general public. The collaboration with ethical hackers allows us to realistically assess the prevailing risks and minimise them as fast as possible.

13 Do only hackers from Switzerland take part?

The ethical hackers are from both Switzerland and abroad. We aim for a good, broad mix of specialist knowledge and the use of collective intelligence.

14 Which other bug bounty programmes are planned? Where can I find more information about this?

Under the Federal Administration's bug bounty programme, additional systems are tested and added to the programme on an ongoing basis. The NCSC reports regularly on the progress of programmes. You can find more information on the NCSC website.

15 Will the bug bounty programme also be offered to public administrations (communes and cantons)?

The NCSC's bug bounty programme is currently available to administrative units in the Federal Administration. We are examining whether and to what extent the service can be offered to the cantons and communes.

16 How are the bug bounty projects financed?

The centralised bug bounty platform and the basic service for running bug bounty programmes in the Federal Administration are financed centrally by the NCSC. The bounties are paid by the department (or administrative unit) running the relevant programme.

17 How long does a bug bounty programme last?

The duration can vary, and is set by the NCSC in consultation with the administrative unit running the programme. The duration can range from a few weeks to a permanent and ongoing programme with no defined end date.

18 What is the difference between private and public bug bounty programmes?

In a private bug bounty programme, participation is by invitation only (taking the above-mentioned admission criteria into account). This means that the definition and size of the participant group is decided by the programme's management.
A semi-private bug bounty programme is visible to the public but no details of the programme are released and participation is dependent on successfully completing the recruitment process (incl. the above-mentioned admission criteria). Here too, the programme's management defines participant numbers.
Public bug bounty programmes are open to all interest specialists and the general public. There are no specific admission criteria.

19 What happens during a bug bounty programme?

In a first step, the bug bounty programme's objectives are set, and the roles and processes are defined. Then a bug bounty programme is set up on Bug Bounty Switzerland AG's bug bounty platform and all the relevant framework conditions are fixed (scope, bounty grid, legal safe harbour, etc.).

If the bug bounty programme is private (see previous question), the selected ethical hackers are invited and the number of participants is successively increased as necessary. The received reports are validated by Bug Bounty Switzerland AG and the NCSC, and are then forwarded to the relevant administrative unit for fixing.

Depending on the requirements, either regular status meetings are held or a simple debriefing to assess the programme takes place upon programme completion.

20 Are ethical hackers allowed to continue searching for vulnerabilities after the end of the bug bounty programme?

The programme guidelines are used to define the timeframe during which ethical hackers may search for vulnerabilities and bounties will be paid. Outside the bug bounty programme guidelines, any vulnerabilities found can be reported at any time through the Coordinated Vulnerability Disclosure process but no bounties will be paid.

21 Are only test environments tested, or do you also test productive systems?

As a general rule, bug bounty programmes are run on productive systems and under realistic conditions in order to ensure the best possible results. In exceptional cases, tests can also be performed on pilot systems or those that are approaching production status. This is decided in collaboration with the relevant administrative unit.

22 To what extent can bug bounty programmes make a strategic contribution to infrastructure security at public administrations and companies?

Every IT system probably still has undetected vulnerabilities. With a bug bounty programme, these can be found quickly and reliably. Collaborating with ethical hackers is a very effective way of improving the security of one's own IT systems. It also increases transparency and public awareness (public trust).

23 Where are the results of bug bounty programmes published?

The results are communicated by the administrative units in consultation with the NCSC. The NCSC regularly publishes the results on the NCSC website. The technical details of the vulnerabilities are not published.