Vulnerability Disclosure Policy

This Vulnerability Disclosure Policy ("policy") has been issued by Livesport s.r.o. with a registered office at Bucharova 2928/14a, Prague 5, Czech Republic, ID no. 274 33 722, registered in the Commercial Register of Municipal Court in Prague, file no. C 113331 ("we" or "us" or "Livesport").

Introduction

At Livesport, we are committed to ensuring security of our systems and user data. We believe that working with the security community can help to identify vulnerabilities in a responsible manner. This Vulnerability Disclosure Policy outlines the guidelines and procedures for reporting security vulnerabilities discovered in our systems.

Bug Bounty Program

We encourage all ethical hackers and computer science enthusiasts to help us in our efforts to keep our systems and data secure. The incentives consist mainly of the Bug Bounty Program ("Bug Bounty Program"), through which we offer financial incentives for reporters of vulnerabilities under conditions stipulated further in this policy.

The Bug Bounty Program runs from November 1, 2023, until we notify of its termination on the https://bugbounty.livesport.eu/ website. We reserve the right to suspend or terminate the Bug Bounty Program at any time without reason, or revoke or change its rules.

Eligibility

The Bug Bounty Program is open to individuals ("participants") who adhere to the terms and conditions outlined in this policy. Whilst we appreciate every report received, only those researchers that meet the following criteria may be eligible to receive a reward and be introduced to the Hall of Fame:

- participants must comply with this policy when discovering vulnerabilities and when submitting a vulnerability report.
- participants must be the first researcher to submit a report concerning a specific vulnerability.
- only vulnerabilities outside of the Out of Scope list submitted through https://bugbounty.livesport.eu concerning Systems in scope will be considered.
- there must be no reason why Livesport s.r.o. would be legally prohibited from rewarding the participant.

Vulnerability reports

Please report security vulnerabilities via https://bugbounty.livesport.eu only, providing all relevant information. The more details you provide, the easier it will be for us to triage, evaluate the report, and fix the issue.
Reports of vulnerabilities submitted via different channels will not be evaluated and/or rewarded.

Systems in Scope

The Bug Bounty Program applies to any of digital assets owned, operated, or maintained by Livesport s.r.o. with *security.txt* referring to https://bugbounty.livesport.eu. However, certain types of vulnerabilities are excluded from the program, as detailed below.

Out of Scope vulnerabilities

- Reports without proof-of-concept exploitation of the vulnerability and potential access to sensitive data of users, third parties, or Livesport s.r.o.
- Physical access attacks to user devices.
- Physical attacks on data center infrastructure or Livesport group's property.
- Attacks on employees or vendors using social engineering techniques.
- Reporting non-existent links on our websites pointing to Livesport group domains.
- Attacks that could cause Denial of Service (DoS) on Livesport group's websites and applications at the application or network layer.
- Creation of duplicate user accounts or accounts without verified ownership of the email address.
- Any form of "non-authenticated" clickjacking or tapjacking.
- Security reports from automated tools.
- Reports about insufficiently secure SSL/TLS ciphers without functional proof-of-concept exploitation against production infrastructure.
- Missing cookie flags.
- Potential vulnerabilities in web forms or applications where no proven exploitation is demonstrated for the purpose of compromising user privacy or gaining unauthorized access to login – autocomplete, missing CSRF tokens, etc.
- Missing SPF or DMARC records.
- XSS attacks that are not stored
- Security threats in unofficial or modified Livesport group applications or the use of devices with violated warranty (e.g., rooted or jailbroken devices).
- Unpatched third-party software components
- Website or application errors that do not clearly have a security nature.

Our Commitments

When working with us, according to this policy, you can expect us to:

- Respond to your report promptly, and work with you to understand and validate your report.
- Strive to keep you informed about the progress of a vulnerability as it is processed according to the internal Vulnerability Handling Process.
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor for your vulnerability research that is related to this policy.

Rewards

Our team of security experts will independently evaluate each reported vulnerability and decide on the amount of the Reward. The decision of the team is final and may not be appealed nor disputed.

The reward structure is defined as follows:

Category	Points	Reward
P1 - Highest	15	up to $2,000
P2 - High	10	up to $1,000
P3 - Medium	7	up to $500
P4 - Low	5	up to $200
P5 - Lowest	3	No financial reward

Points are relevant only for the Hall of Fame which we discuss later in this policy.

Rewards are paid in money via a wire transfer only. Sorry, but we cannot secure other means of money transfer. You may also decide that, instead of sending you the reward, we will donate it to one of the charity fundraisers involved in the Donio program. We cannot split the reward–– you may either take it or donate it.

Employees of Livesport and their immediate family members are not eligible to receive a reward, however, they may decide that the company will donate the amount equal to the reward to a selected charity fundraiser involved in the Donio program.

Rewards may be provided in one of the following currencies: USD, EUR or CZK.
Rewards granted are gross amounts and you are liable for all applicable taxes and duties as a recipient of the amount in your country.

Participants are not entitled to compensation of expenses incurred in connection with their participation in the Bug Bounty Program.

Timelines

Once we receive a report of a vulnerability via https://bugbounty.livesport.eu, our team of security experts will evaluate the report within 30 working days. We will send you an email with our evaluation of your report no later than 35 working days after your submission of the vulnerability report.

In case our security experts decide that you are entitled to a reward, we may also contact you and request payment information (such as a bank account number). We need you to provide us this information within 15 working days, otherwise we will consider you to have waived your right to the reward. Once we receive payment information, we will initiate the wire transfer or the reward to your bank account within the next 15 working days.

We will send emails to notify you and we will initiate the money transfer, however, we cannot be held liable for any defects of delivery services provided by third parties leading to non-delivery or late delivery.

Hall of Fame

We run a Hall of Fame on the https://bugbounty.livesport.eu website. We will publish participants with the highest score, comprised of points gained for reported vulnerabilities, in the Hall of Fame. To have your name in the Hall of Fame, you first need to agree that we can publish your name, or a nickname, there. You can find details in our privacy policy.

Safe Harbor

When conducting vulnerability research, according to this policy, we consider the research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy;
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our Terms of Use that would interfere with conducting security research, and we waive those restrictions on a limited basis;

You are expected, as always, to comply with all applicable laws. If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through https://bugbounty.livesport.eu, or contact us via https://www.livesport.eu/en/contacts before going any further.

Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.

Non-Discrimination

We will not discriminate against security researchers who report vulnerabilities in compliance with this policy. We appreciate your efforts to responsibly disclose any vulnerabilities to us.

Policy Review

This policy is subject to periodic review and may be updated without notice. The most recent version of the policy will be available on https://bugbounty.livesport.eu. All changes to the policy become effective immediately upon their publication on the https://bugbounty.livesport.eu website.

Document change history

Version	Date	Description
1.0	01/11/2023	First issuance.
1.1	29/11/2023	New contact information and minor layout changes.
1.2	30/08/2024	Redefined out-of-scope rule for XSS