Version 1.2, 2023-07-13

Jochen Schweizer mydays Group Bug Bounty Program

General

We, Jochen Schweizer mydays Group, operate a bug bounty program to continuously improve the security of our websites and systems. We welcome reports of vulnerabilities in our websites and take them very seriously. We are willing to pay a reward for specific information that helps us close vulnerabilities in our websites, provided the following conditions are met.

Reporting

Please send all vulnerability reports via email to it-security@jsmd-group.com. A ticket will be created, and you will receive an automatic confirmation of receipt. Please always refer to the ticket number if you need to submit any additional information (or simply reply to the confirmation email).

Vulnerability reports should include a proof of concept that allows us to reproduce the error. Please include screenshots or videos if that helps to better demonstrate the vulnerability.

Non-critical reports are appended to our work queue and processed in the order in which they are received.

Former or current employees of Jochen Schweizer mydays Group or one of its contractors are excluded from the program.

Scope

The following websites are in scope of this program:

- *.jochen-schweizer.de
- *.mydays.de
- *.jsmd-group.com

Not in scope:

- *.regiondo.com
- *.jochen-schweizer-arena.com
- *.jochen-schweizer-group.com
- *.spontacts.com
- *.hip-trips.com
- Any subdomains that are DNS aliases for third party services (e.g., kundenservice.mydays.de or partner.jochen-schweizer.de) and any products for which we cannot fix bugs ourselves (e.g., Atlassian). You can still report vulnerabilities in these services, but we will only forward them to the respective service provider and will not pay any reward.
- A few systems that are at end of life and will be shut down soon (e.g., service.jochen-schweizer.de)

Rules

We ask you to observe the following rules during testing.

- Do not break anything
- Do not leak sensitive data
- Do not perform DOS or DDOS attacks
- Do not disclose vulnerabilities
- Do not use social engineering

Reports will be accepted if the following requirements are met:

- You must be the first reporter of a vulnerability.
- The issue must be of the type of one of the qualifying vulnerabilities listed below.
- The vulnerability must pose an actual risk to us.
- We must be able to reproduce the issue.

Qualifying vulnerabilities

We accept vulnerability reports (depending on our risk assessment) on:

- XSS
- IDOR
- CSRF
- Open redirect
- Information disclosure
- iFrame und HTML injections
- RCE
- SSRF
- Authentication and authorization flaws
- Privilege escalation

We do not accept reports on:

- Clickjacking
- SPF/DKIM/DMARC issues
- Missing or misconfigured HTTP headers and Cookies
- CORS misconfigurations
- TLS misconfigurations
- Potential DOS or DDOS
- Outdated software versions
- And anything that doesn't pose a real risk to us.

Risk assessment

Our security experts will assess the vulnerability and determine the risk to our organization. Please note that we do not judge by CVSS or similar scores alone, but also by the potential impact on our business operations. Reports may be rejected if the assessment showed that there is no or very little risk to us, even if they are on the above list of qualifying vulnerabilities.

Possible Rewards

Rewards will be given at the sole discretion of Jochen Schweizer mydays Group and depend on criticality.

Criticality	Award up to
Critical	500 €
High	200 €
Medium	100 €
Low	50 €
None or very low	0 €

Settlement

As means of payment, we prefer a transfer to a bank account. For transfers to non-EU accounts, we need the SWIFT code of your bank. After accepting a report and promising a reward, we will request an invoice in PDF format from you that must contain the following components:

- Your name
- The date of invoice
- The name and address of the invoice recipient we have given you.
- A short description of the vulnerability and our ticket number as reference, e.g., “Bug bounty for reporting an XSS vulnerability in /partner/bookingwidget, reference ITSEC-123”
- The invoice amount
- Your bank account information

After receiving the invoice, it takes about 4 weeks to go through the approval and payment process.