Coordinated Vulnerability Disclosure (CVD) Policy

The security of our products, systems, and services is important to us. Despite careful development, implementation, configuration, rigorous testing and other security measures, vulnerabilities may still be discovered.

If you have discovered one or more vulnerabilities, you may report them to us confidentially under this policy.

Our goal is to understand, remediate, and – where appropriate – publicly disclose reported vulnerabilities with the help of the reporting person as quickly as possible.

Scope of Application

The scope of this policy covers any reproducible security, design, or implementation issue in our products, web applications, or other services, provided it affects the information security or IT security of our products or the services associated with those products.

Out of Scope

The policy does not apply to the following activities and products and should not be reported under this policy:

- Third-party products and/or services that are not owned or operated by us;
- Misconfiguration on the customer side;
- Improper use;
- Physical attacks on any products;
- Reports resulting from automated scanning tools or automated analyses.

Our Commitment

- Every vulnerability report will be treated confidentially within the applicable legal framework;
- Personal data will not be shared with third parties without your express consent;
- Feedback will be provided for every vulnerability report submitted;
- We will serve as your point of contact for confidential communication throughout the entire process.

Our Expectations

- The discovered vulnerability has not been exploited in an abusive manner;
- No attacks (such as social engineering, spam, (distributed) denial-of-service (DoS), or brute-force attacks, etc.) have been conducted against IT systems or infrastructure;
- No manipulation, compromise, or alteration of any potential systems or data belonging to third parties has been carried out.

Reporting a Vulnerability

To facilitate analysis, reproducibility, and remediation, the report should include the following information:

- A brief description of the vulnerability;
- A description of the potential impact;
- A detailed description of the steps required to reproduce the vulnerability;
- Proof-of-concept code or screenshots;
- An assessment of the severity;
- Where applicable, suggestions for remediation.

In the event of an anonymous report, please note that technical or content-related follow-up queries cannot be answered. Consequently, such vulnerability reports can only be processed to a limited extent or, in some cases, not at all.

To report a vulnerability

Recognition

We appreciate the support of individuals who help us improve our security and would like to publicly recognize researchers in our Hall of Fame.

The publication of a name or other personal data will only take place with the consent of the person concerned.

Safe Harbor

We consider security research conducted in good faith and in accordance with this policy to be authorized.

We will not take legal action in connection with such research, provided the person:

- Complies with this policy;
- Limits testing to the extent necessary;
- Does not manipulate or destroy any data;
- Does not create unnecessary risks for our systems or third parties;
- Reports discovered vulnerabilities promptly and confidentially;
- Keeps the information confidential until an agreed-upon disclosure date.

This policy does not constitute a general authorization for activities outside the defined scope.

Update

This policy is reviewed regularly and may be updated as needed.