Coordinated Vulnerability Disclosure Policy

Coordinated Vulnerability Disclosure Policy

FORMAT Software Service GmbH

The security of our solutions and services is important to us. If you have discovered a potential security vulnerability in a software solution or service provided by FORMAT Software Service GmbH, we would be grateful if you could bring it to our attention.

These guidelines explain how you can report vulnerabilities to us and how we handle such reports.

1 What you can report to us

This policy applies to security vulnerabilities in digital solutions and associated services developed, provided or operated by FORMAT Software Service GmbH, in particular:

- Software solutions from FORMAT Software Service GmbH.
- Web applications and customer portals.
- APIs / interfaces.
- Update, licensing and integration services.
- Other solution-related online services provided by us.

In particular, the following are not covered by this policy:

- Third-party systems or applications that are not operated by us or for which we are not responsible.
- Customer systems without express authorisation.
- Social engineering.
- Physical attacks.
- Denial-of-service tests, load tests or other measures that may impair availability or stability.
- Reports with no apparent security relevance.

2 How to contact us

Please report security vulnerabilities to our central point of contact:

- Reporting channel: Contact form
- Alternative reporting via email: PSIRT@formatsoftware.de

3 What information is helpful

To enable us to review your report quickly, please provide as much specific detail as possible, for example:

- the affected solution or service.
- The version affected.
- Affected URL, function, interface or component.
- A description of the vulnerability.
- Steps to reproduce the issue.
- Potential impact.
- Technical evidence such as screenshots, logs or proof of concept.
- Your contact details in case we need to get in touch.

Even if you do not have all the information to hand, you are of course still welcome to contact us.

4 What we expect from you

We welcome reports made in good faith and with the aim of improving security.

Please note the following in particular:

- Do not access more data than is strictly necessary to demonstrate the vulnerability.
- Do not alter, delete or publish any data.
- Do not carry out any actions that could affect our systems, our customers or third parties.
- Refrain from carrying out automated mass scans, load tests or denial-of-service tests.
- Please do not publish any details until we have agreed on a coordinated disclosure together.

5 What you can expect from us

If you report a security vulnerability to us responsibly, you can expect the following from us:

- We will generally acknowledge receipt of your report within 3 working days.
- We will investigate your report as quickly as possible and contact you if we have any queries.
- We will treat your information confidentially.
- In the case of valid reports, we will keep you informed of the progress of the investigation to an appropriate extent.
- Where possible, we will consult with you regarding any potential disclosure.

If you wish, following agreed disclosure, we will be happy to name you as the whistleblower – naturally, only with your consent.

6 How we handle reports

Upon receipt of your report, we will assess

- whether the reported matter falls within the scope of the policy,
- whether the vulnerability is verifiable/reproducible,
- which solutions, versions or customers might be affected, and
- what risks exist and what measures are required.

We will then prioritise the report, implement immediate internal measures where necessary, and work on a fix or appropriate risk mitigation.

7 Coordinated disclosure

We follow an approach of coordinated vulnerability disclosure.

This means:

- We wish to first investigate reported vulnerabilities and resolve them, or at least effectively mitigate them.
- We then inform affected users in an appropriate manner.
- As a general rule, public disclosure should only take place once this can be done responsibly.

Should an earlier warning be necessary in individual cases for security reasons, we reserve the right to communicate this information at an accelerated pace.

8 Confidentiality and data protection

We treat vulnerability reports as confidential and use the information provided solely for the purposes of reviewing, processing, rectifying, communicating and – where necessary – complying with legal obligations.

Please do not send us any personal data or confidential customer data unless this is necessary to describe the vulnerability.

9 Bug Bounty

FORMAT Software Service GmbH does not currently operate a bug bounty programme.

10 No general authorisation

This policy does not constitute general permission to interfere with our systems, solutions, data or networks. Unlawful acts or acts outside the scope of responsible security testing are not covered by this policy.

11 Changes to this policy

We may update this guideline as necessary, in particular in the event of changes to our solutions, processes or legal requirements.

FORMAT Software Service GmbH
Robert-Bosch-Straße 5
63303 Dreieich
CEO: Horst Scharf

Offenbach Local Court
HRB 32191
VAT: DE 113548293

Phone: +49 6103 9309-0
Fax: +49 6103 9309-9999
info@formatsoftware.de
www.formatsoftware.de

Bank connection: Sparkasse Langen-Seligenstadt
IBAN: DE30 5065 2124 0048 1137 16
BIC: HELADEF1SLS