

COORDINATED VULNERABILITY DISCLOSURE POLICY (CVD POLICY)

Responsible department: CRA-BM

Overview

FRITSCH ("we", "us" or "our") places significant importance on the security of its products, systems and services. We recognise the value of collaboration with the wider security community and appreciate the efforts of all external stakeholders ("the Reporter" or "you"), including customers, partners, and independent security researchers, to identify and responsibly disclose potential vulnerabilities.

This policy explains how you can identify and report vulnerabilities in our products and services. It also ensures that we meet the requirements of the Cyber Resilience Act (CRA).

FRITSCH does not operate a bug bounty programme. Accordingly, by submitting information, the Reporter acknowledges that there is no expectation of financial compensation ("bounties") or non-financial rewards and waives any claim to compensation for submitted information or reports.

By participating in this vulnerability disclosure programme, you agree to comply with the terms set out in this policy and confirm that you have read and understood them.

Products and Services in Scope

This policy applies to all products, systems and services provided or maintained by FRITSCH that fall within the scope of the Cyber Resilience Act (CRA, Regulation (EU) 2024/2847). In addition, the following website and all its subdomains are in scope:

- <https://www.fritsch.de>

Scope of Vulnerability Disclosure

We welcome reports of any security vulnerability that poses a risk to the security of our products, systems or services. This includes, but is not limited to authentication vulnerabilities, authorisation vulnerabilities, information disclosure vulnerabilities or injection attacks. If you wish to report a vulnerability that does not clearly fall within this scope, please contact us first to discuss the matter.

Out of Scope

The following types of reports are outside the scope of this policy and should not be submitted:

- Products or versions that are no longer supported
- Social engineering attacks
- Denial-of-Service (DoS) testing
- Disclosure of software versions
- Clickjacking on non-sensitive pages

Reporting a Vulnerability

Please report vulnerabilities using our Vulnerability Disclosure Form:

https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=Ad3y8OF9wUS_foQhryYfZyPqeK_ikLxHkHPNQDT5YyNUMlpNNFRLTkcXU1MxTUgxMFhKNzZXQk5MWS4u

Reports may also be submitted anonymously.

When reporting a vulnerability, please contact us in English and provide the following information where possible:

- Name and version of the affected product
- Nature of the vulnerability and its impact on the product
- Detailed description of the steps required to reproduce the vulnerability (proof-of-concept scripts or screenshots are helpful)
- Date and time of discovery
- Name and contact details of the reporter (email address and telephone number), unless anonymity is preferred

What We Expect from You

- You must comply with this policy and all applicable laws and regulations.
- Your primary purpose in conducting security research must be the good faith testing, investigation or remediation of a security vulnerability.
- You must not disclose the vulnerability to third parties until we have completed our analysis and remediation activities.
- You may only use exploits to the extent necessary to demonstrate the existence of a vulnerability.
- You must not submit large volumes of low-quality reports.
- You must not be employed by FRITSCH.
- You must not alter or delete data without explicit authorisation.
- You must not conduct Denial-of-Service, social engineering, spam or phishing attacks. Furthermore, you must not test the physical security of FRITSCH facilities.

Safe Harbour

We consider your security research to be authorised and conducted in good faith, and we will not initiate legal action against you, provided that you make reasonable efforts to comply with this policy throughout your research activities. This protection does not apply where there is evidence of criminal intent or unlawful conduct.

Limitation of Liability

All information, updates and remedies provided under this CVD process are supplied on an "as is" basis without any warranty of any kind. To the fullest extent permitted by law, we shall not be liable for any indirect, incidental or consequential damages, or for any loss of profit arising from the exploitation of a reported vulnerability or the application of this CVD policy. This limitation of liability does not apply to damages resulting from willful misconduct, gross negligence, or injury to life, body or health.

What You Can Expect from Us

- We will treat all information you provide as confidential and will not disclose it except where required by law, regulation or other legal obligations.
- We will ensure that your personal data is not shared with third parties without your consent.
- We will acknowledge receipt of your report within five working days, provided that the report was not submitted anonymously.
- We will analyse your report together with the relevant internal teams and keep you informed of progress in good faith.
- We will publicly disclose the vulnerability once our analysis and remediation activities have been completed.

Formal Closure of the Process

A vulnerability case will only be considered formally closed when all the following criteria have been met:

- Remediation: A security update or mitigation measure has been made available to all affected users.
- CRA Notification: All notifications required under Article 14 of the Cyber Resilience Act have been submitted to the relevant CSIRTs and/or ENISA.
- Disclosure: A security advisory, including a CVE where applicable, has been published.
- Documentation: The complete lifecycle of the case has been archived to support regulatory compliance and audit requirements.

Note: We will close a report immediately and without issuing a patch if it is determined to be a false positive or falls outside the scope of this policy.