

COORDINATED VULNERABILITY DISCLOSURE POLICY (CVD POLICY)

Verantwortliche Abteilung: CRA-BM

Übersicht

FRITSCH („wir“ oder „unser“) legt großen Wert auf die Sicherheit seiner Produkte, Systeme und Dienstleistungen. Wir sind uns der Bedeutung der Zusammenarbeit mit der breiteren Sicherheitsgemeinschaft bewusst und schätzen die Bemühungen aller externen Interessengruppen („der Melder“ oder „Sie“) – einschließlich unserer Kunden, Partner und externen Forscher –, potenzielle Schwachstellen zu identifizieren und verantwortungsbewusst offenzulegen.

Diese Richtlinie erläutert, wie Sie nach Schwachstellen in unseren Produkten suchen und diese an uns melden können. Darüber hinaus stellt diese Richtlinie sicher, dass wir die Anforderungen des Cyber Resilience Act (CRA) erfüllen.

Wir führen kein Bug-Bounty-Programm durch. Dementsprechend erkennt der Melder mit der Übermittlung von Informationen an, dass keine Erwartung einer finanziellen Vergütung („Bounties“) oder nicht-finanzieller Belohnungen besteht und dass er auf alle Ansprüche auf Vergütung für übermittelte Informationen oder Meldungen verzichtet.

Durch die Teilnahme an diesem Programm zur Offenlegung von Sicherheitslücken erklären Sie sich damit einverstanden, die in dieser Richtlinie beschriebenen Bedingungen einzuhalten, und bestätigen, dass Sie diese gelesen und verstanden haben.

Betroffene Produkte und Dienstleistungen

Diese Richtlinie gilt für alle von FRITSCH bereitgestellten oder gewarteten Produkte, Systeme und Dienste, die unter die CRA-Verordnung (Cyber Resilience Act, EU-Verordnung 2024/2847) fallen. Darüber hinaus fallen die folgenden Websites und deren Subdomains in den Geltungsbereich:

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

Umfang der Offenlegung von Sicherheitslücken

Wir freuen uns über jede Meldung einer Sicherheitslücke, die eine Gefahr für die Sicherheit unserer Produkte, Systeme oder Dienste darstellt. Dazu gehören unter anderem Sicherheitslücken im Zusammenhang mit Authentifizierung, Autorisierung, Datenoffenlegung und Injektionsangriffen. Sollten Sie eine Sicherheitslücke melden wollen, die nicht unter diesen Geltungsbereich fällt, kontaktieren Sie uns bitte zunächst, um dies zu besprechen.

Ausnahmen vom Geltungsbereich

Die folgenden Meldungen fallen nicht in den Geltungsbereich dieser Richtlinie und können nicht eingereicht werden:

- Produkte oder Versionen, für die kein Support mehr angeboten wird
- Social-Engineering-Angriffe
- Denial-of-Service-Tests
- Offenlegung von Softwareversionen
- Clickjacking auf nicht sensiblen Seiten

Berichterstattung

Bitte melden Sie Sicherheitslücken über das Formular zur Meldung von Sicherheitslücken unter

https://forms.cloud.microsoft/Pages/ResponsePage.aspx?id=Ad3y8OF9wUS_foQhryYfZyPqeK_ikLxHkHPNQDT5YyNUMlpNNFRLTkcxU1MxTUgxMFhKNzZXQk5MWS4u

Meldungen können auch anonym eingereicht werden.

Wenn Sie eine Sicherheitslücke melden, kontaktieren Sie uns bitte auf Englisch und geben Sie folgende Informationen an:

- Name und Version des betroffenen Produkts
- Art der Sicherheitslücke und ihre Auswirkungen auf das Produkt
- Detaillierte Beschreibung der Schritte, die zur Reproduktion der Sicherheitslücke erforderlich sind (Proof-of-Concept-Skripte oder Screenshots sind hilfreich)
- Datum und Uhrzeit der Entdeckung
- Name des Meldenden und Kontaktdaten (E-Mail-Adresse, Telefonnummer) – es sei denn, Sie möchten anonym bleiben

Was wir von Ihnen erwarten

- Sie sind verpflichtet, diese Richtlinie sowie alle geltenden Gesetze und Vorschriften einzuhalten.
- Ihr vorrangiges Ziel bei der Sicherheitsforschung muss das in gutem Glauben durchgeführte Testen, Untersuchen oder Beheben einer Sicherheitslücke sein.
- Sie dürfen die Sicherheitslücke erst dann an Dritte weitergeben, wenn wir unsere Analyse und Behebung abgeschlossen haben.
- Sie dürfen Exploits nur in dem Umfang einsetzen, der zum Nachweis des Vorliegens einer Sicherheitslücke erforderlich ist.
- Sie dürfen keine großen Mengen an Berichten von geringer Qualität einreichen.
- Sie dürfen nicht bei FRITSCH beschäftigt sein.
- Sie dürfen Daten nicht ohne ausdrückliche Genehmigung ändern oder löschen.
- Sie dürfen keinerlei Denial-of-Service-, Social-Engineering-, Spam- oder Phishing-Angriffe durchführen. Darüber hinaus dürfen Sie die physische Sicherheit der Einrichtungen von FRITSCH nicht testen.

Safe harbor

Wir betrachten Ihre Sicherheitsforschung als zulässig und ethisch vertretbar und werden keine rechtlichen Schritte gegen Sie einleiten, sofern Sie sich im Rahmen Ihrer Sicherheitsforschung nach bestem Wissen und Gewissen bemühen, diese Richtlinie einzuhalten. Dies gilt nicht, wenn erkennbare kriminelle Absichten verfolgt wurden oder werden.

Haftungsbeschränkung

Alle im Rahmen dieses CVD-Verfahrens bereitgestellten Informationen, Aktualisierungen oder Korrekturen werden „wie besehen“ und ohne jegliche Gewährleistung bereitgestellt. Wir übernehmen keine Haftung für indirekte, zufällige oder Folgeschäden sowie für entgangene Gewinne, die sich aus der Ausnutzung einer gemeldeten Sicherheitslücke oder der Anwendung dieser CVD-Richtlinie ergeben. Diese Haftungsbeschränkung gilt nicht für Schäden, die durch vorsätzliches Fehlverhalten, grobe Fahrlässigkeit oder durch Verletzung von Leben, Körper oder Gesundheit verursacht werden.

Was Sie von uns erwarten können

- Wir behandeln alle von Ihnen gemeldeten Informationen vertraulich und geben sie nicht weiter, es sei denn, dies ist aufgrund von Gesetzen, Vorschriften oder Bestimmungen erforderlich.
- Wir stellen sicher, dass Ihre personenbezogenen Daten ohne Ihre Einwilligung nicht an Dritte weitergegeben werden.
- Wir bestätigen den Eingang Ihrer Meldung innerhalb von 5 Werktagen – sofern Sie die Meldung nicht anonym abgegeben haben.
- Wir werden Ihre Meldung gemeinsam mit den zuständigen Teams analysieren und Sie nach bestem Wissen und Gewissen auf dem Laufenden halten.
- Wir werden die Sicherheitslücke öffentlich bekannt geben, sobald wir unsere Analyse und Behebung abgeschlossen haben.

Formeller Abschluss des Verfahrens

Ein Sicherheitslückenfall gilt erst dann als offiziell abgeschlossen, wenn die folgenden Kriterien erfüllt sind:

- Behebung: Ein Sicherheitsupdate oder eine Abhilfemaßnahme steht allen betroffenen Nutzern zur Verfügung.
- CRA-Meldung: Die gemäß Art. 14 CRA vorgeschriebenen Meldungen an CSIRTs/ENISA wurden vollständig übermittelt.
- Offenlegung: Ein Sicherheitshinweis (ggf. mit CVE) wurde veröffentlicht.
- Dokumentation: Der gesamte Lebenszyklus des Falls wird zur Einhaltung gesetzlicher Vorschriften und zur Vorbereitung auf Audits archiviert.

Hinweis: Wir schließen einen Bericht sofort und ohne Patch, wenn sich herausstellt, dass es sich um einen Fehlalarm handelt oder der Fall außerhalb des Geltungsbereichs liegt.