

Coordinated Vulnerability Disclosure Policy

1. Purpose

The security of our products matters to us. Despite careful development and testing, vulnerabilities cannot be ruled out entirely. We therefore ask security researchers, customers, partners and anyone else who discovers a vulnerability to report it to us confidentially, so that we can fix it before it harms others.

This policy describes how to report a vulnerability to us, what you can expect from us and what we ask of you. It is based on the international standards ISO/IEC 29147 and ISO/IEC 30111 and on the requirements of Regulation (EU) 2024/2847 (Cyber Resilience Act).

2. Scope

This policy applies to vulnerabilities in the hardware, firmware and software products of Pyramid Computer GmbH, in particular the Akhet, Polytouch and Faytech product lines, including the firmware and software we provide.

The company website and the internal IT systems of Pyramid Computer GmbH are not covered. [Please send reports concerning these to the address below as well; we will forward them internally.]

If your finding concerns a third-party component (e.g. processor, BIOS base, operating system), we will pass the information on to the respective manufacturer and keep you informed of the status where possible.

3. How to report a vulnerability

Please send your report by email to:

psirt@pyramid.de

This address is monitored by our Product Security Incident Response Team (PSIRT). Reports may be submitted in German or English.

We do not currently provide a published key for encrypting reports. If you would like to send confidential details in encrypted form, please first send us a short message without technical details; we will then agree on a suitable channel with you.

The following information helps us to process your report:

- the affected product with its type designation and, if known, the firmware or software version
- a description of the vulnerability and its potential impact
- steps to reproduce the vulnerability (with a proof of concept, if available)
- whether the vulnerability is already publicly known or is already being exploited
- your contact details for follow-up questions and whether and how you would like to be credited in a later acknowledgement

Please do not send any personal data of third parties or customer data that is not necessary to describe the vulnerability.

4. Our process and commitments

Once we have received your report, we proceed as follows:

1. Acknowledgement: We confirm receipt of your report within [3] working days.
2. Initial assessment: Within [10] working days, we let you know whether we were able to reproduce the vulnerability and how we provisionally classify it.
3. Evaluation: We rate the severity using the Common Vulnerability Scoring System (CVSS) and determine how urgently it needs to be fixed.
4. Remediation: We develop and test a fix or an interim solution (workaround), where necessary in coordination with the manufacturers of affected components.
5. Status updates: We keep you informed of our progress, at least every [30] days.
6. Publication: As soon as a fix is available, we inform our customers through a security advisory and make the update available.

In accordance with the Cyber Resilience Act, we provide security updates without delay and free of charge.

5. Coordinated disclosure

We ask you not to publish details of the vulnerability before a fix is available and our customers have had the opportunity to install it. The standard period is 90 days from the acknowledgement of your report. For complex fixes, for example where several manufacturers are involved, we will agree on an extension with you.

If a vulnerability is already being actively exploited, we act immediately without waiting for the standard period. In this case, Article 14 of the Cyber Resilience Act also requires us to notify the competent authorities (the coordinating CSIRT and ENISA) within short deadlines. We only share personal data about the reporting person where this is necessary or required by law.

6. What we ask of you

Please observe the following principles in your security research:

- Act in good faith and with the aim of improving security.
- Only test devices that you own or are authorised to test. Do not test any of our customers' systems without their consent.
- Do not access more data than is strictly necessary to demonstrate the vulnerability, and do not share or modify such data.
- Avoid tests that impair the availability of systems (e.g. denial-of-service attacks).
- Do not carry out social engineering attacks against our employees, customers or partners, or physical attacks on our sites.
- Give us reasonable time to fix the vulnerability before you publish any information.

7. Legal safe harbour

Anyone who complies with this policy when searching for and reporting vulnerabilities is, in our view, acting in good faith. In such cases, Pyramid Computer GmbH will not take legal action against the reporting person. This assurance does not apply to actions that intentionally cause damage or violate applicable law, and it does not bind third parties, in particular customers or law enforcement authorities.

8. Recognition

If you wish, we will credit you in our security advisory as the person who discovered the vulnerability. We do not currently offer a bug bounty programme or financial reward.

9. Security advisories for customers

Published security advisories for our products can be found on our website under “Product Security – Security Advisories”.

10. Data protection

We process personal data submitted with a report solely to handle the report and to fulfil our legal obligations. Further information can be found in our privacy policy.

11. Changes

We review this policy regularly and update it as needed. The current version is always available at this address.

Pyramid Computer GmbH

Bötzingen Strasse 60,
79111 Freiburg, Germany

Your PSIRT team