Information regarding CyberSecurity

Vulnerability Handling at MEIKO

Introduction

MEIKO is grateful for all the leads it receives concerning security risks and processes them conscientiously and transparently. By uncovering any vulnerabilities, we can provide our customers with a constant high level of security. It is therefore in our interest to identify any weak points and develop a satisfactory solution.

This vulnerability disclosure policy outlines the procedure to be followed when reporting any vulnerability to us (the "Organization") and when examining our products for weaknesses. We recommend reading this vulnerability disclosure policy fully before you report vulnerability and always act in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures.

The reporting party

The reporting party is responsible for its own actions and must observe the principles of proportionality as well as subsidiarity when investigating and reporting vulnerabilities. In other words, the reporting party should not do more than necessary to demonstrate the vulnerability and should always report the vulnerability to the system/information owner first.

In return, if you follow the instructions of this policy, the organization will not take any legal action against your wellmeant vulnerability investigations and reports. This legal protection does not apply if there is evidence of malicious intent.

The reporting party must
- report the problem as soon as possible to prevent malicious parties from discovering the vulnerability and taking advantage of it.
- make the report to the organization in a confidential manner to prevent others from gaining access to this information.

The reporting party and the organization make clear agreements on the disclosure of the vulnerability. If more than one organization is involved, the basic principle is that the vulnerabilities can only be published if all organizations agree to this fact.

Reporting

If you believe you have found a security vulnerability, please submit your report to us using the following email: service-support@meiko-global.com

Only emails written in English or German can be considered.

Please include the following vulnerability details in your report:

- Asset (web address, IP Address, product or service name) where the vulnerability can be observed
- Weakness (e.g. CWE) (optional)
- Severity (e.g. CVSS v3.1) (optional)
- Title of vulnerability (mandatory)

- Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations) (mandatory)
- Impact (what could an attacker do?) (mandatory)
- Steps to reproduce. These should be a benign, nondestructive, proof of concept.

Optional Contact Details:
- Name
- Email Address

What to expect

After you have submitted your report, we ensure that the report reaches the department that is best suited according to our processes. After submission, the process is as following:
- The organization sends an acknowledgement of receipt to the reporting party.
- The report is evaluated and handled according to our risk assessment (impact, severity, complexity of exploitation).
- The organization will keep the reporting party informed about the status
- The reporting party should refrain from inquiring more often than once every 14 days
- The organization will publish the findings in consultation with the reporting party, if there is a reasonable probability that the vulnerability is also present in other places.
- We will handle your report with strict confidentiality
- We will not pass on your personal details to third parties without your permission.

Guidance

Do NOT:
- Take advantage of the vulnerability or problem you have discovered, for example through unnecessary access, excessive or significant amounts of data
- Reveal the problem to others until it has been resolved
- Modify data in the Organization's systems or services
- Use attacks on physical security, social engineering, distributed denial of service, spam or highintensity invasive or destructive scanning tools to find vulnerabilities
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests
- Disrupt the Organization's services or systems

Contact

Email: service-support@meiko-global.com