Promicon Elektronik GmbH + Co. KG
Im Michelreis 6
72124 Pliezhausen

Fon +49 (0) 7127-9 37 30
www.promicon.de

TLP:CLEAR

Policy on Coordinated Vulnerability Disclosure

1 Introduction

At Promicon Elektronik GmbH + Co. KG (furthermore refered as Promicon or Promicon Systems), the safety of its products and services is the top priority. We are committed to adhering to security standards that protect our customers' privacy and data integrity.

To ensure the security of our customers' systems and our products, we ask the reporter to engage in coordinated disclosure. In addition, to treat the information as confidential until a solution is found, rather than immediately disclosing vulnerabilities on public platforms.

Our Product Security Incident Response Team (furthermore refered as Promicon PSIRT) is committed to addressing all reports promptly to ensure the continued reliability and security of Promicon products.

This policy on the coordinated disclosure of vulnerabilities describes the process for reporting vulnerabilities to us and explains what reporters can expect in return.

Please read this policy in its entirety before reporting a vulnerability, and always act in accordance with it.

2 Scope

This policy applies to all active products created by Promicon, regardless of their contractual status or stage in the product lifecycle—whether they are in the development phase, the maintenance phase, or even after maintenance has ended.

In the interest of responsible disclosure, we ask that you refrain from the following scenarios:

- Physical attacks, social engineering or other non-technical vulnerability tests
- Network Denial of Service (DoS or DDos) attacks or tests, that impair or damage availability
- A huge number of automated scans
- Vulnerability reports in third-party software or services that are not under our control

If you are unsure whether a test falls within the scope, please consult with us beforehand.

The Promicon PSIRT's responsibilities are fully supported by management and are in the company's best interests.

Policy on Coordinated Vulnerability Disclosure

3 Reporting Vulnerabilities

Vulnerabilities may already have been addressed through patches, new versions, or clarifications regarding their non-exploitability. Please check in advance to see if you are up to date on this matter.

If you believe you have found a potential vulnerability in one of our systems, please report it to the Promicon PSIRT via email:

psec-psirt@promicon-systems.de

To enable the Promicon PSIRT to address the potential vulnerability, please provide the following information.:

- Full product name and the affected component
- Hardware and software version numbers for all components involved
- Date and time of the incident (please specify the time zone)
- Detailed description of the vulnerability
    - Technical details (such as system configuration, log data, and a description of the exploit/attack code)
    - Detailed step-by-step guide to reproducing the vulnerability
    - Attachments that help reproduce the issue, such as images, videos, scripts, and payloads
    - Proof-of-Concept code, if availbale
- Assessment of the severity of the vulnerability
- Impact of the vulnerability, including how an attacker could exploit it
- Your contact information—we respect anonymous reports

The information should be provided in German or English.

Insufficient information may result in the Promicon PSIRT being unable to confirm the information.

Promicon recommends that the person submitting the report encrypt any sensitive information sent via email. The Promicon PSIRT supports messages encrypted using the OpenPGP standard. Please send us your PGP key so that Promicon PSIRT can reply to you securely.

In addition, the Promicon PSIRT can be reached by phone at +49 (0) 71 27 - 9 37 30.

Promicon PSIRT's business hours are generally limited to standard office hours. These are:

9:00 a.m. – 4:00 p.m. (GMT+0100 and GMT+0200 in summertime) from Monday to Friday, except during the school holidays in Baden-Württemberg, Germany and company holidays.

Policy on Coordinated Vulnerability Disclosure

You can find our public PGP key and its corresponding fingerprint on our website:

https://www.promicon.de/en/promicon-psirt.html

https://www.promicon-systems.de/en/promicon-psirt.html

https://www.varimotion.de/en/promicon-psirt.html

https://www.compactmotion.de/en/promicon-psirt.html

https://www.vari-move.de/en/promicon-psirt.html

https://www.promicon.com/en/promicon-psirt.html

https://www.promicon-systems.com/en/promicon-psirt.html

https://www.vari-motion.de/en/promicon-psirt.html

https://www.compact-motion.de/en/promicon-psirt.html

Important Information

- We process only information regarding potential vulnerabilities affecting Promicon products.
- Anonymous reports can only be processed to a limited extent, or possibly not at all, because there is no way to ask follow-up questions regarding technical details or content.
- We will use your contact information solely for the purpose of analyzing and identifying potential vulnerabilities. Your contact information will only be shared with third parties with your express permission.
- To protect our customers, we ask that you not disclose this vulnerability to other individuals or organizations without first consulting with the Promicon PSIRT.

4 Response times

If you decide to share your contact information with us, we are committed to communicating with you as openly and promptly as possible. However, we ask for your understanding that it may take some time for us to respond.

- We will confirm receipt of your report within five business days.
- We will do our best, within our capabilities, to confirm the existence of the vulnerability and to communicate to you as transparently as possible the steps we are taking to resolve it, including any issues or challenges that may delay a solution.
- We will engage in an open dialogue with you to discuss any issues.

Policy on Coordinated Vulnerability Disclosure

5 Safe-Harbor

Promicon will not take legal action against individuals who discover and report vulnerabilities in accordance with this policy, provided that they:

- does not cause harm to Promicon, our customers, or others
- that compromises the privacy or security of our customers or the operation of our services
- not violate criminal laws
- Details about vulnerabilities will not be released until Promicon has confirmed that the corrective measures have been completed

6 Recognition

Promicon does not operate a bug bounty program. By providing data and information regarding a vulnerability, you acknowledge that no expectation of payment is associated with such provision and that you expressly waive any future claims for payment against Horscht in connection with your provision of such information.

Although Promicon does not offer a bug bounty program or any other form of compensation, it recognizes and appreciates the contributions of security researchers.

Changes to this policy

Promicon reserves the right to change this policy at any time without prior notice. We recommend that you check this page regularly for updates.

Should difficulties of interpretation arise, the German text of this policy shall be binding.

Subject to technical changes.