

Information on Cyber Security

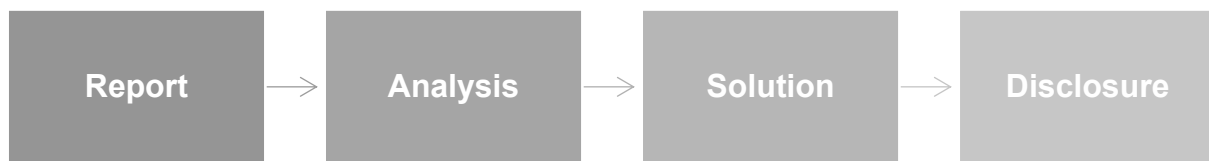
Vulnerability Handling at VEGA

VEGA Grieshaber KG is grateful for all leads it receives concerning security risks and processes them conscientiously and transparently. Reports regarding vulnerabilities usually come from researchers, customers, industry groups, CERTs, partners or the general public. 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.

During the entire process, we strive to work together with all parties involved in a trusting and professional manner.

Of course we always respect the interests of the reporting party. To promote transparency, the entire vulnerability handling process is described in this document. If you have any questions about vulnerability handling at VEGA, please contact us at psirt@vega.com. Communication with the person reporting can take place via the security platform CERT@VDE.

The vulnerability disclosure will also be available at CERT@VDE and on our homepage. Further information regarding our partner can be found on their website.



Report

If you discover a security gap in our systems, we ask you to report it to us immediately. We undertake to respond to your report within one working day. If you do not receive a response, please contact us again.

Only e-mails written in English or German can be considered. Es können nur E-Mails berücksichtigt werden, die in den Sprachen Englisch oder Deutsch verfasst sind.

Vulnerability reports should be sent to psirt@vega.com. Should you wish to encrypt your message, you can do this via CERT@VDE.

If you would like to send us a larger amount of data, we also offer a data transfer service. You can get more detailed information via this link: <https://transfer.vega.com/>

We ask you to include the following information in your report:

- The affected system/software + version number
- A detailed description of the vulnerability
- Status of the vulnerability disclosure
- Preferred communication channel for queries and updates

Alternatively, you have the option of reporting the vulnerability via CERT@VDE. Information about CERT@VDE is available at <https://cert.vde.com>



Analysis

The incoming report is first checked and analysed by us. It is then forwarded to the appropriate department. If we need further information, we contact the person reporting.

Solution

Our PSIRT carries out the vulnerability handling process together with the department responsible for the product. Other parties can also be involved in this process.

The solution to the reported vulnerability is communicated to the reporter.

Disclosure

The vulnerability is disclosed at an agreed time. All required information, including the remedial measures taken, are disclosed then. Provided we have consent from the person who reported, he/she will be acknowledged on our website for their cooperation.

Contact

E-mail: psirt@vega.com

Phone: +49 7836 50-0

09.09.2021