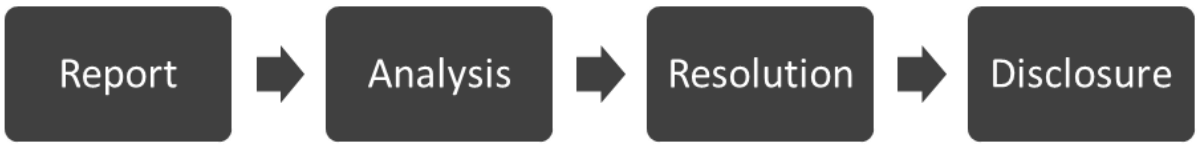
Vulnerability handling at Pepperl+Fuchs

Pepperl+Fuchs investigates all reports of security vulnerabilities affecting Pepperl+Fuchs products and services. We welcome vulnerability reports from researchers, customers, industry groups, CERTs, partners or from the general public and will respect the interests of the reporting party. We strongly urge reporting parties to perform a coordinated disclosure, as immediate public disclosure may cause a '0-day situation' which puts our customers' systems at unnecessary risk.

If a security vulnerability is reported to Pepperl+Fuchs, it will be handled according to the following process:



Report

To report a vulnerability, please send an email to cert@pepperl+fuchs.com.

We ask that you include as much of the information below as possible.

- Type of issue (buffer overflow, cross-site scripting, etc.)
- Detailed description of vulnerability, including proof-of-concept, exploit code or network traces (if available)
- Affected product and version
- Disclosure status of the vulnerability (Was it already publicly disclosed?)

For encrypted communication, our public PGP key can be downloaded from
http://www.pepperl-fuchs.com/cgi-bin/db/doci.pl?ShowDocByDocNo=DOCT-5119
fingerprint: B6F2 3233 F5AA 5753 515C 4976 22F0 14F8 9335 5E7B

We commit to responding within one business day. If for some reason you do not receive a confirmation within that time frame, please follow up with us to ensure that we received your original message.

Only emails composed in English or German can be considered.

If a large amount of data needs to be submitted, we are glad to offer a service for data transfer.

Analysis

We will investigate and attempt to reproduce the vulnerability. If required, we may request more information from the reporting party.

After the analysis, we inform the party about the outcome and, if necessary, agree on a joint approach.

Resolution

Pepperl+Fuchs conducts internal vulnerability resolution. Other parties that are involved in the vulnerability may be contacted during this process. Regular communication is maintained to the reporting party about the status. Pre-releases of patches may be provided to the reporting party for verification.

Disclosure

Pepperl+Fuchs is committed to a coordinated disclosure. For all vulnerabilities that have been adequately fixed a security bulletin will be published at

www.pepperl-fuchs.com/cybersecurity

Where the situation demands a security advisory may be released describing mitigation procedures before a patch is available.

An advisory or bulletin will typically include the following information:

- Description of the vulnerability
- Affected products and software/hardware versions
- Information on mitigating factors and workarounds
- Availability of patches
- With the reporting party's consent, credit is provided