

Coordinated vulnerability disclosure policy

Document control

- Owner: PLAST-CONTROL GMBH
- Last Modified: 28.08.2026
- Review cycle: Annually

Purpose and Scope

This policy defines the process for handling vulnerability reports (coordinated vulnerability disclosure, CVD) affecting products developed by PLAST-CONTROL GMBH.

Vulnerability definition

A 'vulnerability' means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat.

The following requirements are considered for a vulnerability to be valid:

- The vulnerability affects one of our products or services in scope.
- The vulnerability report relates to publicly unknown information.
- The vulnerability report may not be a result of automated tools or scans without supporting documentation.

Reporting Channels and Communication

Vulnerability reporting information guidance is available on the company web site in these locations:

- www.plastcontrol.de/report-a-vulnerability
- www.plastcontrol.de/.well-known/security.txt

The following contact options are accepted:

- product-security@plastcontrol.de

The reporter should use an encrypted and digitally signed email for the transmission of confidential information.

Vulnerability report details

Reporters are encouraged to include in vulnerability reports, if possible,

- the affected products and tested versions,
- how the vulnerability was discovered (including any tools used),
- any information indicating active exploitation,
- proof-of-concept (PoC) code or instructions showing how the vulnerability can be exploited, and
- if and how they want to be publicly acknowledged for the report.

Communication

Good communication is important for vulnerability reports. Further explanations and documentation may be required, especially in the case of complex issues. If technical or content-related queries are not responded to, the corresponding vulnerability report can only be processed to a limited extent or possibly not at all.

Assurance to vulnerability reporters

PLAST-CONTROL GMBH commits to the following:

- We will treat each incoming vulnerability report confidentially to the extent permitted by law. Information required for the public disclosure of the vulnerability is exempt.
- We will not disclose personal data of the reporter without explicit consent.
- We will respond to each submission or update of a vulnerability report within the guaranteed response times.
- We will not pursue criminal charges against the reporter if this policy and its principles have been complied with by the reporter. This does not apply if recognizable criminal intentions have been or are being pursued.
- We will be available as a contact for a trustful exchange throughout the entire CVD process.
- We will not require the reporter to sign a non-disclosure agreement (NDA).

Code of conduct for reporters

To only reward reporters with no malicious intent, the following behaviour is expected of reporters.

- No abuse of the reported vulnerability by the reporter. No damage has been caused beyond the reported vulnerability.
- No attacks (such as social engineering, spam, (distributed) DoS or "brute force" attacks, etc.) were carried out against our IT systems or infrastructures by the reporter.
- No manipulation, compromise or modification of possible systems or data of third parties was carried out by reporter.
- No tools for exploiting vulnerabilities have been offered, e.g. on darknet markets, by the reporter for a fee or free of charge that third parties could use to commit crimes.
- No unacceptable behaviour, e.g. discrimination, sexism or insults.

Reports from non-compliant entities are still treated to the best extent possible.

Response times

Vulnerability report submissions or updates are acknowledged by a human within five working days. Vulnerabilities are assessed and detailed feedback is given within a further five working days. Detailed feedback includes at least either

- a statement of the manufacturer as to whether it confirms or rejects the reported vulnerability,
- meaningful queries to understand the reported vulnerability, or
- an explanation why the investigation of the reported vulnerability is taking longer, along with a commitment to provide an update within a further ten working days.

These response times do not apply if a vulnerability was reported anonymously.

Vulnerabilities are remediated within

- 7 days for severity critical (9.0-10.0),
- 30 days for severity high (7.0-8.9),
- 60 days for severity medium (4.0-6.9), and
- 90 days for severity low or none (0.0-3.9).

Vulnerabilities are publicly disclosed within 90 days. In exceptional circumstances, the periods until remediation and public disclosure can be extended further.

Validated and verified vulnerabilities are publicly disclosed as stated in the security.txt file.

End of process

The CVD process is considered complete under any of the following conditions:

- if the indications of the vulnerability report are unfounded.
- if the reporter fails to respond to technical or content-related queries for at least 30 days and therefore the corresponding vulnerability report can only be processed to a limited extent or not at all.
- if the vulnerability has been mitigated or fixed by an appropriate patch and has been publicly disclosed.
- if the vulnerability has been publicly disclosed and will no longer be mitigated or fixed.

The end of the CVD process is communicated to the reporter (unless the vulnerability was reported anonymously).