Helmholz®
COMPATIBLE WITH YOU

Helmholz PSIRT: Vulnerability Handling and Disclosure Process

Version 1 en

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.de

29.11.2023

Content

1 Introduction

Our commitment to security is paramount and we are actively committed to quickly assessing and resolving security concerns. The Helmholz “Product Security Incident Response Team” (PSIRT) aims to minimize the risk associated with security vulnerabilities for our customers.

Helmholz is a manufacturer of components for industrial communication. The products must therefore be considered in a holistic security approach in a machine or production plant and, if necessary, supplied with security updates.

We continuously strive to ensure the safe usability of Helmholz products by providing timely information, assistance and effective elimination of security vulnerabilities in our products, software and applications.

The Helmholz PSIRT acts as a central team within Helmholz GmbH & Co. KG for managing the testing and disclosure of potential vulnerabilities. Any reports of potential vulnerabilities or other security incidents related to Helmholz products can be reported or forwarded to the Helmholz PSIRT.

Upon receipt of a report, we will immediately deploy the necessary resources to analyze and validate the issue and take appropriate remedial action.

The Helmholz PSIRT coordinates and maintains communication with all parties involved, both internally and externally, to be able to react appropriately to identified security problems.

The Helmholz PSIRT actively monitors relevant communication channels to be promptly informed about potential security vulnerabilities in all software packages used.

In cooperation with our partner CERT@VDE, Helmholz PSIRT coordinates the response and disclosure of all externally identified product vulnerabilities. Our vulnerability handling and disclosure process comprises the following four steps:

1. Report
2. Analysis
3. Processing
4. Disclosure

1.1 Purpose of this document

The clear purpose of this document is to make our approach to security incidents and vulnerabilities transparent and to strengthen collaboration with our customers, users, and partners.

It is important to Helmholz that users have a consistent and clear source that helps them understand how Helmholz responds to such incidents and helps the user to manage security issues.

2 Report

Anyone can report security vulnerabilities, regardless of the existence of contracts, the product's end-of-life status, or whether they are a Helmholz customer or user.

Helmholz welcomes vulnerability reports from researchers, industry groups, CERTs, partners, and any other source. Helmholz does not require a non-disclosure agreement for receiving reports.

Helmholz respects the interests of the reporting party (including anonymous reports if requested) and agrees to address any vulnerability that can be reasonably believed to be related to Helmholz products.

Helmholz urges reporting parties to report in a coordinated manner, as immediate public disclosure would result in a "zero-day situation" that would unnecessarily jeopardize the systems of Helmholz's customers.

To report a vulnerability affecting a Helmholz product, please contact the Helmholz PSIRT team using the contact information below.

- E-Mail: psirt@helmholz.de
- Notification via the Helmholz Coordinator CERT@VDE: https://cert.vde.com

Please report the following information:

- Description of the vulnerability, including proof-of-concept, exploit code or network protocols (if available)
- Affected product including model and firmware version (if available)
- Awareness of the vulnerability (has it already been publicly disclosed?)
- Approval or rejection (anonymous report) of the reporting party's contribution to the public disclosure of the vulnerability in the Helmholz Security Advisory (if published)

Communication by e-mail to the Helmholz PSIRT can be secure and encrypted. S/MIME, PGP key and further information about the PSIRT can be found here:
https://www.helmholz.de/service-support/service/security-psirt/

2.1 Handling of contact details of reporter

If the Helmholz PSIRT receives a vulnerability report classified as serious, the contact details of the reporter will be added to the reporting database if they are not already available. The reporting database is maintained based on the provisions of the GDPR. The contact details are used to contact and communicate with the reporter. Contact details of reporters with whom Helmholz has not communicated in the last 3 years will be deleted.

Further information on data protection can be found here: https://www.helmholz.de/datenschutz

3 Analysis and verification

The Helmholz PSIRT examines and analyzes all reports regardless of the software version or the status of the product life cycle until the product has reached the "Last Day of Support" (LDoS).

Helmholz checks the relevance and applicability to Helmholz products and requests further information from the notifier if necessary.

3.1 Classification of vulnerabilities

Helmholz evaluates and classifies vulnerabilities on the basis of a qualitative representation (e.g. low, medium, high and critical) in order to support the correct evaluation and prioritization in the Helmholz vulnerability management process.

Helmholz takes the following parameters into account:

- the potential impact of the vulnerability
- public knowledge about the vulnerability
- whether there are published exploits for the vulnerability
- the volume of deployed products that are affected
- the availability of an effective workaround instead of a patch

4 Processing

Helmholz carries out internal vulnerability processing in cooperation with the responsible development groups. CERT@VDE, as a partner of the Helmholz PSIRT, is informed in advance of a security problem and supports the Helmholz PSIRT in the evaluation and development of CVEs and advisories if necessary.

During this time, regular communication takes place between Helmholz and the reporting party to provide information on the current status and to ensure that the manufacturer's position is understood by the reporting party. If available, preliminary versions of software corrections and safety instructions can be provided by Helmholz to the reporting party for review.

4.1 Remediation

We take security issues seriously and strive to assess and resolve them in a timely manner. Once the issue has been successfully analyzed and if a vulnerability fix is required, appropriate fixes are developed and prepared for distribution. The timeline for remediation depends on many factors, such as severity, the affected product, the current development cycle, the product lifecycle and whether the issue can only be fixed in a major release.

The remedies may take one or more of the following forms:

- A new release of the software/firmware
- A patch/update provided by Helmholz
- Instructions for installing an update or patch from a third-party provider
- A workaround to mitigate the vulnerability

Regardless, we do not guarantee a specific solution to problems and not all identified problems can be resolved.

5 Disclosure

Helmholz uses the Helmholz Security Advisories via CERT@VDE and software release notes via Helmholz's own channels for the publication of vulnerabilities.

For vulnerabilities with a "high" or "critical" rating, Helmholz will publish an advisory via CERT@VDE.

For vulnerabilities with a rating of "low" or "medium", Helmholz will provide information via software release notes.

Helmholz reserves the right to deviate from these guidelines in individual cases if additional factors are not recorded correctly and an advisory is not published.

5.1 CVE numbering

Helmholz applies for a CVE number (Common Vulnerabilities and Exposures) if a reported vulnerability is based on the code or an implementation of Helmholz. The CVE number itself is assigned by our responsible CVE numbering office CERT@VDE.

Helmholz only assigns a CVE number for reported vulnerabilities if these vulnerabilities have been confirmed by Helmholz in cooperation with CERT@VDE or if they are contained in a third-party component used by Helmholz.

5.2 Helmholz Advisory

Helmholz Security Advisories provide detailed information about security issues that directly affect Helmholz products and require an upgrade, fix or other customer action - e.g. a workaround.

Helmholz Security Advisories are used to disclose vulnerabilities with a "high" or "critical" rating.

The Helmholz Security Advisories are published on the website of CERT@VDE:
https://cert.vde.com/de/advisories/vendor/helmholz

A Helmholz Security Advisory usually contains the following information:

- Description of the vulnerability with CVE reference and CVSS score
- Identity of products and software/hardware versions known to be affected
- Information on mitigating factors and workarounds
- The location of the available firmware, update or patch download
- With the consent of the reporting party, the reporting party will be named and acknowledged for reporting and cooperation

5.3 Software release notes

Software release notes are used to disclose "medium" and "low" severity issues. In the software release notes, customers can receive new information such as version changes, new features, fixed bugs, a CVE ID, etc. regarding their products.

The software release notes are published on the Helmholz website next to the product.

5.4 Customer notification

In most cases, Helmholz intends to notify customers when a practical workaround or fix for a vulnerability has been identified.

Helmholz will utilize existing customer notification processes to manage the release of patches. This may include a direct customer notification, the public release of a security advisory or an entry in the software release notes with all necessary information.

This will be published after the PSIRT has completed the vulnerability handling and disclosure process and determined that sufficient software patches or workarounds are available or a subsequent release of fixes to address the vulnerabilities is planned.

If the Helmholz PSIRT has observed an active exploitation of a vulnerability that could result in an increased risk to Helmholz customers, Helmholz will expedite the release of a security advisory. The notification may or may not include a patch or workaround.

Exceptions may be made on a case-by-case basis to improve communication for a particular document.

Helmholz therefore uses the following communication channels, depending on the degree of severity:

- Publication via CERT@VDE
- Newsletter
- Direct e-mail to customers who have purchased the affected product