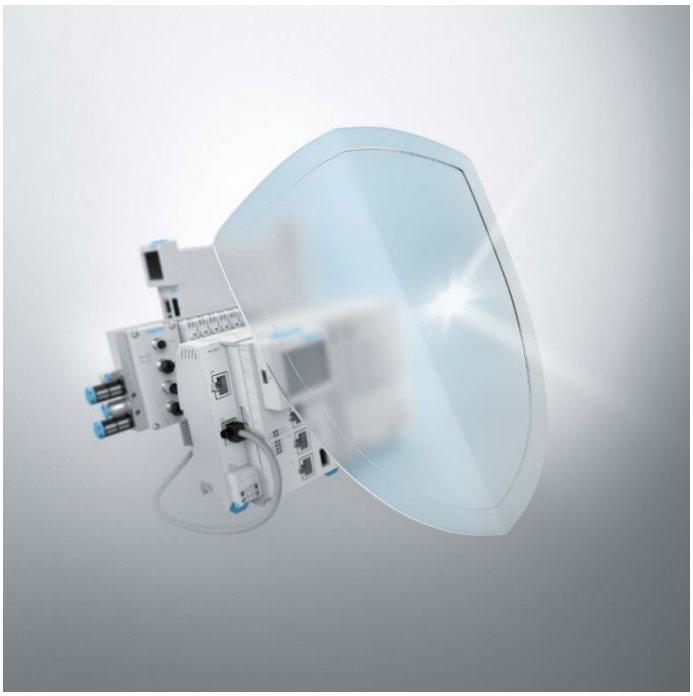
Festo PSIRT
Product Security Incident Response Team

Festo PSIRT - Vulnerability Handling & Disclosure Process



Vulnerability Handling & Disclosure Process

Date
September 8th, 2021

Creator
TP-D/TPF

Version
1.2

Festo SE & Co. KG

www.festo.com/psirt
psirt@festo.com
Ruiter Straße 82
73734 Esslingen
GERMANY

Festo Vulnerability Handling & Disclosure Process

1. 1 Introduction

We take security concerns seriously and work to quickly evaluate and address them. The goal of the Festo Product Security Incident Response Team (PSIRT) is to minimize customer risk associated with security vulnerabilities by providing timely information, guidance, and remediation of vulnerabilities in our products, including software and applications. Festo PSIRT is the central team of the Festo SE & Co. KG for managing the testing and disclosure of security vulnerabilities. All reports about possible weak points or other security incidents in connection with Festo products can be forwarded to the Festo PSIRT. The Festo PSIRT adheres also to ISO/IEC 29147:2014.

Once reported, we commit the appropriate resources to analyze, validate and provide corrective actions to address the issue. The Festo PSIRT coordinates and maintains communication with all parties involved, internal and external, in order to be able to react appropriately to identified security problems.

The Festo PSIRT coordinates the response and disclosure of all externally identified product vulnerabilities.

The vulnerability handling and disclosure process consists of the following four steps at Festo, see figure 1:

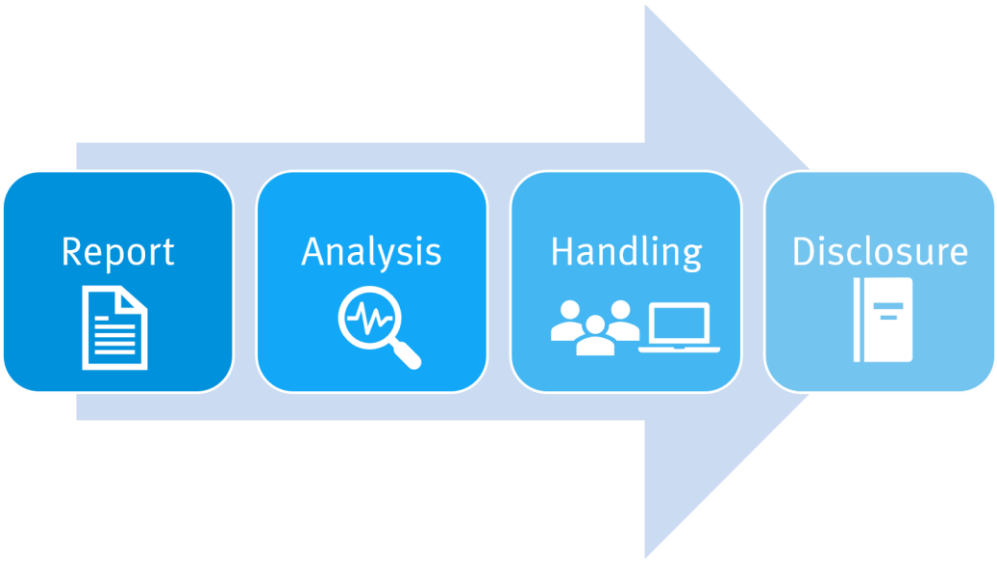


Figure 1

1. 2 Purpose

This policy was created for customer guidance and information in the event of a reported vulnerability in a Festo product or service. It is essential to ensure that Festo customers have a consistent, unambiguous resource to help them to understand how Festo responds to events of this nature.

1. 3 Report

Everyone is encouraged to report discovered vulnerabilities, regardless of service contracts or product lifecycle status. Festo welcomes vulnerability reports from researchers, industry groups, CERTs, partners, and any other source as Festo does not require a nondisclosure-agreement as a prerequisite for receiving reports. Festo respects the interests of the reporting party (also anonymous reports if requested) and agrees to handle any vulnerability that is reasonably believed to be related to Festo products. Festo urges reporting parties to perform a coordinated disclosure, as immediate public disclosure causes a ‘0-day situation’ that unnecessarily endangers Festo's customer systems.

To report a security vulnerability affecting a Festo product, please contact the Festo PSIRT using the provided contact options below.
The contact points at Festo are:

- E-Mail: psirt@festo.com
- Contact form on https://www.festo.com/psirt
- Reporting through the Festo Coordinator CERT@VDE: https://cert.vde.com/

Please report the following information:

- Description of the vulnerability, including proof-of-concept exploit code or network traces (if available)
- Affected product including model and firmware version (if available)
- Publicity of vulnerability (was it already publicly disclosed?)
- Consent for acknowledge the reporter's contribution in the public announcement of the vulnerability in the Festo Security Advisory (if published).

More information about the PSIRT can be found here: https://www.festo.com/psirt

1. 3. 1 Handling of contact details of the reporters

If the Festo PSIRT receives a vulnerability report that is deemed to be serious, the contact details of the reporter, if not already available, are added to the reporter database. The maintenance of the reporter database is based on the regulations of the GDPR (General Data Protection Regulation [German: DSGVO: Datenschutz-Grundverordnung]). For example, the contact data of reporters with whom Festo has not communicated in the last 3 years will be deleted.

The contact information is used to get in contact and communicate with the reporter. In addition, it can be used to be mentioned in the advisory as reporter or in a hall of fame on request.

Data protection statement by Festo SE & Co. KG | Festo Corporate: https://www.festo.com/group/en/cms/10195.htm

1. 4 Analysis and Verification

Festo investigates and analyzes the validity of the vulnerability. Relevance and application to Festo products will be verified and if needed, Festo will request more information from the reporter.

1. 4. 1 Classification of Festo vulnerabilities

Festo evaluates and classifies vulnerabilities based on a qualitative representation (e.g., low, medium, high, and critical) to help properly assess and prioritize in Festo vulnerability management processes. The Qualitative representation is defined as the Festo Security Impact Rating (SIR).

If there is a vulnerability in a third-party software component that is used in a Festo product, Festo PSIRT derive the SIR based on a severity score provided by the component creator in context of Festo to reflect the impact to Festo products. Per default, the SIR medium is be assigned to the vulnerability till adjusted by Festo PSIRT to account for Festo-specific variables like,

- the potential impact of the vulnerability;
- public knowledge of the vulnerability;
- whether published exploits exist for the vulnerability;
- the volume of deployed products that are affected; and
- the availability of an effective mitigation in lieu of the patch.

1. 5 Handling

Festo performs internal vulnerability handling in collaboration with the responsible development groups. CERT@VDE having a partnership with Festo PSIRT may be notified about a security issue in advance. During this time, regular communication is maintained between Festo and the reporting party to inform about the current status and to ensure

that the vendor's position is understood by the reporting party. If available, pre-releases of software fixes and Festo Security Advisories may be provided to the reporting party for verification.

1. 5. 1 Types of Remediation

We take security concerns seriously and work to evaluate and address them in a timely manner. After the issue was successfully analyzed and if a fix is necessary to cope with the vulnerability, corresponding fixes will be developed and prepared for distribution. Response timelines will depend on many factors, including the severity, the product affected, the current development cycle, QA cycles and whether the issue can only be updated in a major release.

Remediation may take one or more of the following forms:

- A new release
- A Festo-provided patch, update, or new version of the software/firmware
- Instructions to download and install an update or patch from a third-party
- A workaround to mitigate the vulnerability

Notwithstanding the foregoing, we do not guarantee a specific resolution for issues and not all issues identified may be fixed.

1. 6 Disclosure

Festo uses the Festo Security Advisory and Software Release Notes for the publication of vulnerabilities. In the following, the types of publication are described in more detail. Festo reserves the right to deviate from these guidelines in specific cases if additional factors are not properly captured and not disclose an advisory.

There are two publication types for a remediation. Independent of the SIR assessment, the vulnerability is published via a Festo Security Advisory or via Software Release Notes. The following table shows the publication types and when Festo will request a CVE number.

Festo Security Impact Rating (SIR)	CVE required	Type of publication
Critical	yes	Festo Security Advisory
High		
Medium (default)	no	Release Note
Low / Informational	no	

1. 6. 1 CVE numbering authority CERT@VDE

Festo requests a Common Vulnerabilities and Exposures (CVE) number, if a reported vulnerability is based on Festo's own code or implementation. The CVE number itself is issued and handled as a service by our responsible CVE numbering authority CERT@VDE.

Note: Festo does not assign CVE identifiers for reported vulnerabilities until such vulnerabilities have been confirmed by Festo or they are in a used 3rd party component.

1. 6. 2 Festo Security Advisory

Festo Security Advisories provide detailed information about security issues that directly involve Festo products and require an upgrade, fix or other customer action. Festo Security Advisories are used to disclose vulnerabilities with an SIR score high or critical.
The Festo Security Advisories will be published, e.g. at the website of CERT@VDE (https://cert.vde.com/de-de/advisories.)
A Festo Security Advisory usually contains the following information:

- Description of the vulnerability with CVE reference and CVSS score
- Identity of known affected products and software/hardware versions
- Information on mitigating factors and workarounds

- The location of available fixes
- With the consent of the reporting party, credit will be provided for reporting and collaboration.

1. 6. 3 Software Release Notes

Software Release Notes are used to disclose issues with a medium and informational/low severity. In the Software Release Notes, customers can obtain new information such as version change, new functions, fixed bugs, a CVE ID. etc. regarding their products.

1. 6. 4 Customer Notification

In most cases, Festo intends to notify customers when there is an identified practical workaround or fix for a security vulnerability. Festo will use existing customer notification processes to manage the release of patches, which may include direct customer notification, public release of a Festo Security Advisory or an entry in the Software Release Notes containing all necessary information. This will be posted after the PSIRT has completed the vulnerability handling & disclosure process and determined that sufficient software patches or workarounds exist, or subsequent public disclosure of code fixes is planned to address the vulnerabilities.
If the Festo PSIRT has observed active exploitation of a vulnerability that could lead to increased risk for Festo customers, Festo will accelerate the publication of a security announcement describing the vulnerability that may or may not include a complete set of patches or workarounds.

The following table summarizes the methods used to notify customers about the aforementioned security publications. Exceptions may be made on a case-by-case basis to increase communication for a given document.

Publication	E-Mail	CERT@VDE	External Portal (Festo Support Portal)
Festo Security Advisory	Yes	Yes	Yes
Software Release Note	No	No	Yes

1. 7 Definitions

PSIRT: A team of individuals who are responsible for addressing security issues found in a product or service. Depending on the circumstances, this might be a formal security team from an organization, a group of volunteers on an open-source project, or an independent panel of volunteers (such as the Internet Bug Bounty).

Finder: Anyone who has investigated a potential security issue in some form of technology, including academic security researchers, software engineers, system administrators and even casual technologists.

Report: A Finder's description of a potential security vulnerability in a particular product or service. Reports always start out as non-public submissions to the Festo PSIRT.

Vulnerability: A software bug that would allow an attacker to perform an action in violation of an expressed security policy. A bug that enables escalated access or privilege is a vulnerability. Design flaws and failures to adhere to security best practices may qualify as vulnerabilities.

CVE: CVE is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE Entries are comprised of an identification number, a description and at least one public reference.