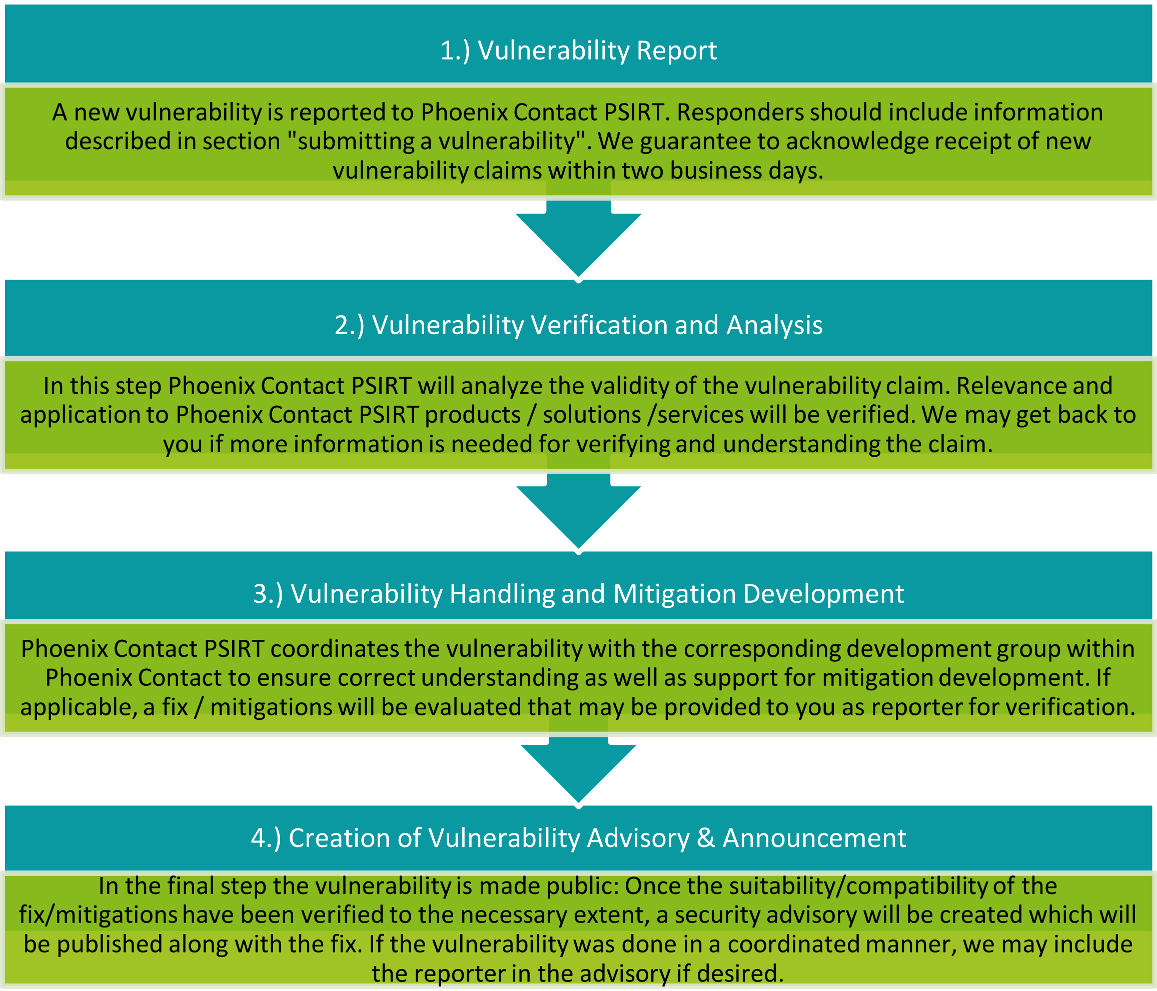
Vulnerability handling process at Phoenix Contact

1. Security Vulnerability Handling at Phoenix Contact

In order to encourage parties to contact us with vulnerability claims, we would like to make the steps transparent that are involved in responding to a vulnerability claim at Phoenix Contact PSIRT, as well as describing when Phoenix Contact PSIRT will issue a security advisory.

2. Phoenix Contact PSIRT Security Vulnerability Handling Process

All vulnerability claims are handled according to the following procedure and steps:



1.) Vulnerability Report

A new vulnerability is reported to Phoenix Contact PSIRT. Responders should include information described in section "submitting a vulnerability". We guarantee to acknowledge receipt of new vulnerability claims within two business days.

2.) Vulnerability Verification and Analysis

In this step Phoenix Contact PSIRT will analyze the validity of the vulnerability claim. Relevance and application to Phoenix Contact PSIRT products / solutions /services will be verified. We may get back to you if more information is needed for verifying and understanding the claim.

3.) Vulnerability Handling and Mitigation Development

Phoenix Contact PSIRT coordinates the vulnerability with the corresponding development group within Phoenix Contact to ensure correct understanding as well as support for mitigation development. If applicable, a fix / mitigations will be evaluated that may be provided to you as reporter for verification.

4.) Creation of Vulnerability Advisory & Announcement

In the final step the vulnerability is made public: Once the suitability/compatibility of the fix/mitigations have been verified to the necessary extent, a security advisory will be created which will be published along with the fix. If the vulnerability was done in a coordinated manner, we may include the reporter in the advisory if desired.

...

3. Security Vulnerability Disclosure Policy

For fixes to security vulnerabilities in Phoenix Contact products, solutions and services, Phoenix Contact PSIRT will issue a standardized security advisory informing about the security vulnerability in detail, describing affected components as well as which mitigations/available fixes are available for mitigating associated risks.

If you have any further questions with regards to our vulnerability handling process, please contact us at psirt@phoenixcontact.com.

4. Security Advisories issued by Phoenix Contact PSIRT

This section of the Phoenix Contact PSIRT website contains all security advisories that were issued by Phoenix Contact PSIRT, grouped by year of issuance.

Phoenix Contact PSIRT issues security advisories according to a predefined standardized structure, with the following elements:

Element name:	Element content and explanation of purpose:
Advisory Title:	A self-explanatory name summarizing the vulnerability and the product.
Advisory ID:	A unique number identifying the advisory.
Revision History:	A version history documenting initial publication and later changes to the advisory.
Vulnerability description:	A descriptive explanation of the vulnerability which helps parties to understand the characteristics of the vulnerability as well as the vulnerability type.
Affected products/solutions/services:	Product / solutions / services that are confirmed to be affected by the vulnerability.

...

Impact:	Description of what the impact of the vulnerability is, if exploited. The impact may have security-related elements (such as e.g. data corruption) but also non-security related elements, depending on the underlying system.
Classification of Vulnerability:	This section contains a classification of the vulnerability according to the methodology of the Common Vulnerability Scoring System (CVSS) version 3. Both the overall score in numbers (e.g. 5.3) as well as the detailed vector used for score calculation are being disclosed here.
Temporary fix / mitigation:	Any factors and options existing that could be used for reducing / mitigating the risks associated with the vulnerability are provided here. This may include workarounds or mitigating/compensating factors to consider in the environment
Remediation:	Actual fixes in the form of software updates / patches which have been created by the developing groups.
Reference information and disclaimer:	Any additional references which may help in understanding the vulnerability, e.g. links to other websites. Legal disclaimer for security advisories. Contact information for Phoenix Contact PSIRT.
Acknowledgement:	Acknowledgement for vulnerability coordination / reporting efforts of the reporting party (if applicable).