DURAG GROUP

Guideline

CP-III.4-03-00-P

Vulnerability Handling and Disclosure Guideline

Content

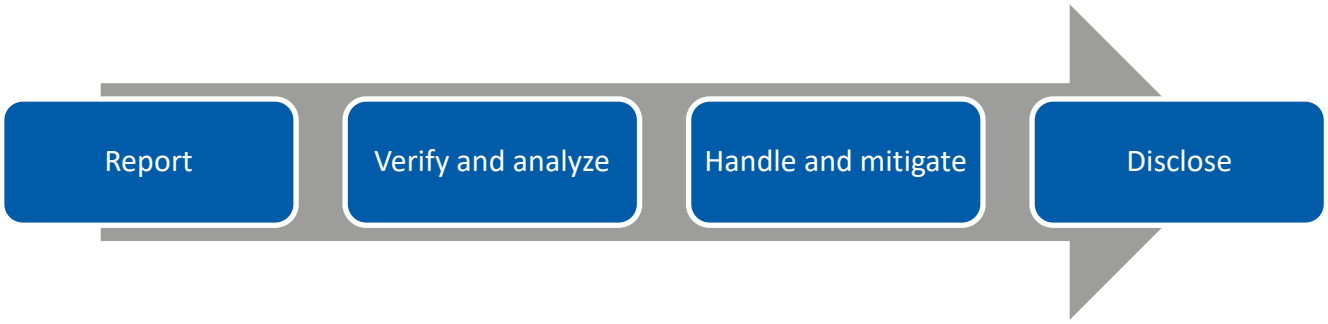
1 Introduction and Purpose

We take security concerns seriously and work to quickly evaluate and address them. DURAG is committed to helping customers minimize risks associated with security vulnerabilities in its products. The goal of the DURAG Product Security Incident Response Team (PSIRT) is to provide customers with timely information, guidance, and mitigation of vulnerabilities in our products, solutions and services. DURAG PSIRT is the central team of the DURAG GmbH for managing the response to and disclosure of security vulnerabilities. DURAG cooperates for this purpose with CERT@VDE, the first platform for the coordination of IT security vulnerabilities in the field of automation. All reports about possible vulnerabilities or other security incidents in connection with DURAG products, solutions and services can be forwarded to the DURAG PSIRT or CERT@VDE.
Once reported, we commit the appropriate resources to analyze, validate and provide corrective actions to address the issue. The DURAG PSIRT / CERT@VDE coordinates and maintains communication with all parties involved, internal and external, in order to be able to react appropriately to identified security problems.
This guideline was created for customer guidance and information in the event of a reported vulnerability in a DURAG product, solution or service.

Vulnerability detection is seen as a joint effort by a wide range of parties, with the aim of consistently providing our customers with a high level of security. This is particularly important since DURAG products, solutions and services fulfill important protective functions and are used in critical infrastructures. In order to encourage all parties to report vulnerabilities in a coordinated manner, the process is transparently described in this document. Throughout the entire process, the DURAG PSIRT strives to work in a trusting and professional manner with all parties involved.
If there are any questions regarding this document, please contact the DURAG PSIRT at psirt@durag.com. Contact can be made in German or English.

2 DURAG Security Vulnerability Handling and Disclosure Process

In order to encourage parties to contact DURAG GROUP with vulnerability claims, we would like to make the steps transparent that are involved in responding to a vulnerability claim at DURAG PSIRT, as well as describing when DURAG PSIRT will issue a security advisory.
The vulnerability handling and disclosure process consists of the following four steps at DURAG:



2.1 Report

The DURAG PSIRT welcomes vulnerability reports from anyone, regardless of any customer status, and investigates them diligently. Reporters include security researchers, academia, CERTs, business partners, government agencies, industry associations, and suppliers. For submitting a vulnerability report neither a non-disclosure agreement (NDA) nor any other contract is necessary or prerequisite.
A new vulnerability is reported to DURAG PSIRT. Reporters should include information described at https://www.durag.com/psirt when reporting a vulnerability. We guarantee to acknowledge receipt of new vulnerability claims within seven days.
Alternatively vulnerabilities can be reported to DURAG PSIRT via CERT@VDE using the email address info@certvde.com or using the web form https://certvde.com/helper/reportvuln/.
The DURAG PSIRT and CERT@VDE are in close exchange on highest confidentiality level and inform each other about new reports. The further processing is accompanied and supported by the CERT@VDE.

2.2 Verify and analyze

In this step DURAG PSIRT will analyze the validity of the vulnerability claim. Relevance and application to DURAG products / solutions /services will be verified. DURAG PSIRT or CERT@VDE might get back to the reporter if more information is needed for verifying and understanding the claim.
Subsequently, the vulnerability claim will be forwarded to the corresponding departments and analyzed. A regular communication with the reporter will be in place.

2.3 Handle and mitigate

DURAG PSIRT coordinates the vulnerability with the corresponding department within DURAG to ensure correct understanding as well as support for mitigation development. The responsible departments will develop a solution to handle the risk of the vulnerability appropriately. If applicable and technically possible, a fix / mitigation will be evaluated that may be provided to the reporter for verification.

2.4 Disclose

In the final step the vulnerability is made public at a coordinated time and a security advisory will be created. If the vulnerability was done in a coordinated manner, we may include the reporter in the advisory if desired.
For security vulnerabilities in DURAG products, solutions and services, DURAG PSIRT in cooperation with CERT@VDE 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. The DURAG Security Advisories are published in human readable format on the CERT@VDE website: https://certvde.com/en/advisories/vendor/durag/. DURAG Security Advisories are also published in machine-processable CSAF format.

DURAG reserves the right to deviate from these guidelines in specific cases if additional factors are not properly captured, i.e. security impact rating, and not disclose an advisory.
If there are any further questions with regards to our vulnerability handling process, please contact us at psirt@durag.com.