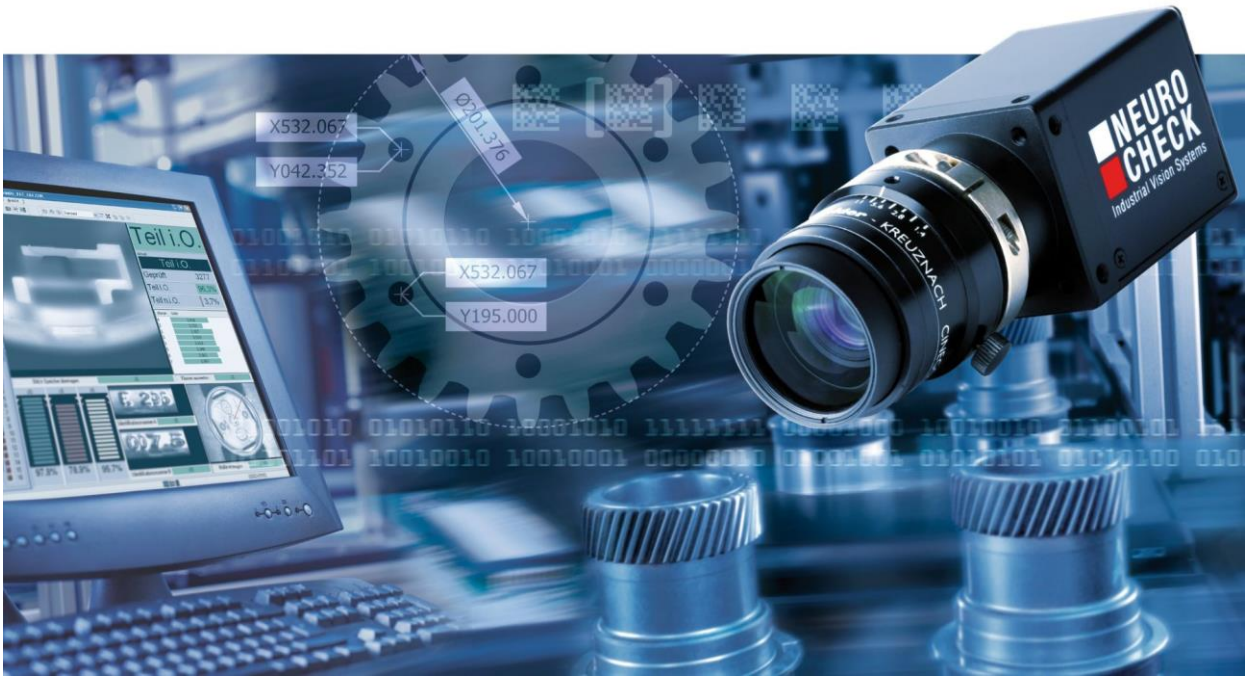


PSIRT-VDP

Vulnerability Disclosure Policy

Management System	PSIRT Management System
Document Category	External Document
Version	V02
Status	Released
Confidentiality	Public
Document Owner	CRA Compliance Officer
Creation Date	2026-11-04
Approval Date	2026-11-05
Approving Authority	Executive Management

Revision History

Version	Date	Description of Changes	Changed by
01	2026-07-29	Initial document creation	Andre Lucke
02	2026-11-04	Content clarifications	Andre Lucke

Contents

1 Introduction 3

2 Reporting Product Vulnerabilities 3

3 Information Required for Vulnerability Reports 3

4 Handling of Vulnerability Reports 4

5 Coordinated Vulnerability Disclosure 4

6 Guidance for Vulnerability Reporters 4

1 Introduction

NeuroCheck takes the security of its products seriously and welcomes the responsible disclosure of potential product vulnerabilities. This Vulnerability Disclosure Policy (VDP) describes how security researchers, customers, and other individuals can report suspected or confirmed product vulnerabilities to us. For the purposes of this policy, the term product vulnerability refers to security vulnerabilities and other security-relevant defects in our products.

This policy applies to products developed by NeuroCheck or distributed under its own product responsibility. Third-party products that NeuroCheck merely resells are not covered by this policy. Vulnerabilities in such products should be reported directly to the respective manufacturer.

If you suspect or discover a security vulnerability in one of our products, we encourage you to inform us. We will promptly review all incoming reports and assess whether remediation measures are necessary.

2 Reporting Product Vulnerabilities

Please use the following email address exclusively to report product vulnerabilities:

security@neurocheck.com

It serves as the Single Point of Contact (SPoC) for reporting product vulnerabilities to NeuroCheck. This helps ensure that your report reaches the responsible PSIRT directly and can be processed as quickly as possible.

3 Information Required for Vulnerability Reports

Please describe the product vulnerability as clearly and comprehensively as possible, including sufficient technical details to allow us to assess it. Each report should include the following information:

- Affected product and version number
- Unique product identification (e. g. license number, serial number, or project number)
- Detailed description of the product vulnerability
- System environment and steps to reproduce
- Impact and/or risk
- Contact information for follow-up questions

Optional but highly helpful information may include:

- Proof of concept
- Logs / screenshots
- CVSS assessment
- Workarounds

We reserve the right to discontinue processing a report if the information provided does not allow for an adequate review and assessment of the product vulnerability.

4 Handling of Vulnerability Reports

Upon receiving a report of a product vulnerability, we will take the following steps:

- We will acknowledge receipt of every report without undue delay.
- We will carefully review and assess each reported product vulnerability.
- We will keep you reasonably informed about the progress of the handling process.
- We will treat all information provided as confidential and use it solely for the purpose of handling the reported product vulnerability. Information will only be shared to the extent necessary for analyzing and remediating the product vulnerability or as part of coordinated disclosure.
- We will coordinate the disclosure of confirmed product vulnerabilities in accordance with the principles of Coordinated Vulnerability Disclosure (CVD).
- We reserve the right to determine the nature and scope of appropriate remediation measures at our sole discretion. The provision of security updates is governed by the respective product lifecycle and our Product Lifecycle Policy.
- We will not pursue legal action against individuals who report product vulnerabilities in good faith, responsibly, and in accordance with this policy.

5 Coordinated Vulnerability Disclosure

Please do not disclose any information about a reported product vulnerability until we have had the opportunity to review and assess the product vulnerability and prepare appropriate remediation measures. We aim to coordinate the disclosure of confirmed product vulnerabilities with you in accordance with the principles of Coordinated Vulnerability Disclosure (CVD). Upon request, you will be appropriately credited when the product vulnerability is publicly disclosed, using your name or a pseudonym.

If no agreement on disclosure can be reached, we reserve the right to inform customers and, where applicable, the competent authorities about the product vulnerability. NeuroCheck may also publish product-related security information. Any such disclosure will be limited to what is necessary to safeguard product security or required by law.

6 Guidance for Vulnerability Reporters

Please conduct only security research that does not adversely affect our systems or those of our customers. In particular, you must not carry out denial-of-service (DoS) attacks, including distributed denial-of-

service (DDoS) attacks, engage in other activities that impair the availability of services, access personal data, or undertake any activities that violate applicable law.

We do not operate a bug bounty program. By submitting a vulnerability report, you expressly acknowledge that such a report does not entitle you to any reward or other compensation from NeuroCheck.

When submitting a vulnerability report, you grant NeuroCheck a royalty-free right to use the information and materials provided as part of the vulnerability report for the purpose of analyzing and remediating the product vulnerability, improving product security, and internally documenting and publishing security-related information. This includes sharing such information and materials with third parties where necessary for these purposes.

We would like to thank everyone who contributes to the security of our products by responsibly reporting product vulnerabilities.