

VULNERABILITY DISCLOSURE POLICY

Introduction

As the leading European vendor of Networks and Cybersecurity products, we support vulnerability disclosure as an essential process. As part of this goal, a standardized process and clear guidelines for conduct are essential to achieving meaningful outcomes quickly, efficiently, and for the greatest possible benefit of our customers.

In this process, we value all contributions from customers, partners, researchers, and institutions as part of a global collaborative effort to make our world a safer place.

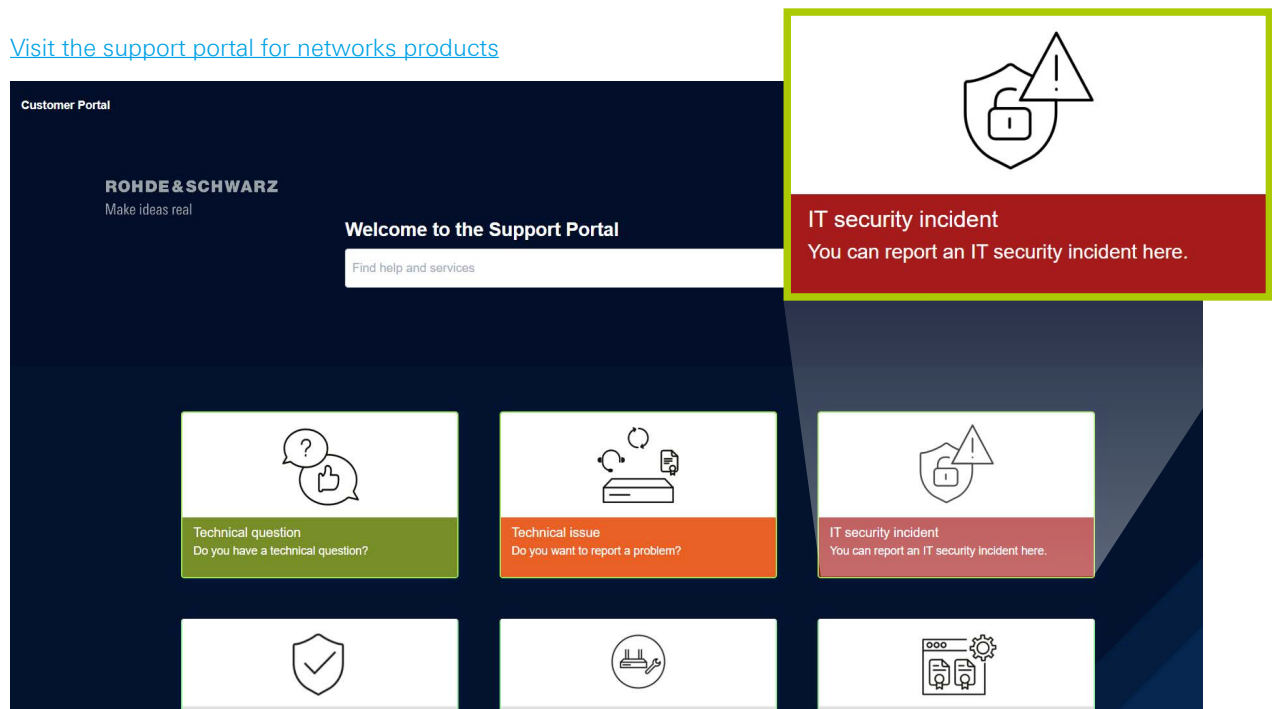
The following document highlights how the process works for customers (this page) and all other parties (next page).

Submitting a vulnerability or product security incident via customer support channels

Network products (formerly LANCOM)

As a customer you may generate a ticket with the ticket type security incident in our portal. Login to the portal and generate the ticket.

[Visit the support portal for networks products](#)



Cybersecurity products (formerly RSCS)

Login to the portal and generate a general ticket. Mark in the ticket as “security relevant” - YES.

[Visit the support portal for Cybersecurity products](#)

Submitting a vulnerability or product security incident via e-mail

We value your contribution to security. Please note that Rohde & Schwarz Networks and Cybersecurity GmbH does not participate in any formal bug bounty programs.

Please submit your findings via email to: security.rs-nc@rohde-schwarz.com ([OpenPGP](#))

To ensure the secure exchange of information, we prefer using encrypted communication. The required key information is contained in rs-nc.rohde-schwarz.com/.well-known/security.txt.

You may alternatively request the OpenPGP and S/MIME certificates for security.rs-nc@rohde-schwarz.com via our secure portal at: <https://securemail.rohde-schwarz.com/>.

If the information is classified or secret (e.g., VS), please let us know. We will provide a secure mechanism for submitting the data to us.

The following information helps us expedite the process:

- ▶ Your contact details (e-mail, telephone number, address)
- ▶ Products in question, including exact firmware versions and other relevant details
- ▶ Your CVSS score assessment (3.1 or higher)
- ▶ Technical details and background of your findings (proof-of-concept etc.)
- ▶ Relevant background information, including whether you are employed by one of our customers

Public recognition and compensation

Submitting a vulnerability report does not create any entitlement to compensation, rewards, recognition, or reimbursement of expenses. Rohde & Schwarz Networks and Cybersecurity GmbH may, at its discretion, acknowledge researchers who responsibly report valid security vulnerabilities. Public recognition is not guaranteed and may depend on factors such as report quality, impact, responsible conduct, and legal or customer confidentiality requirements.

Processing a vulnerability report

Confirmation of receipt

We will typically acknowledge receipt of your report by the next business day in North Rhine-Westphalia, Germany, and no later than seven days after submission. The report will undergo an initial review to filter out spam before being forwarded to the responsible team for further processing.

Assessment and clarifications

The assessment process consists of the following stages:

- 1. Pre-assessment:** Specialists assess the report, its potential impact, and criticality.
- 2. Incident creation:** If the findings are confirmed, we open an incident, assign a tracking number, and determine whether further action is required.
- 3. Follow-up:** We contact you to clarify any outstanding questions, discuss additional findings, and coordinate remediation and disclosure timelines.

Fixing

If we determine that the issue requires remediation, we will take all necessary steps to develop a solution as quickly as possible. During this process, we strive to provide you with regular updates. Overall, we aim to resolve the issue within 90 days.

General communication and closure

If required, we get in touch with the relevant authorities and institutions, such as:

- **The German Federal Office for Information Security (BSI)** if BSI-certified products are affected or reporting is required under the NIS2 Directive.
- **The European Union Agency for Cybersecurity (ENISA)** if reporting is required under the Cyber Resilience Act (CRA).
- **A CVE Numbering Authority (CNA)** if a CVE identifier needs to be assigned to the reported vulnerability. Following remediation, including the implementation of fixes or workarounds (if applicable), and the completion of all other necessary preparations, we may contact you to discuss a potential publication date.

Public disclosure and communication guidelines

As a final step, we typically publish a public statement on our website and close the incident. All publicly disclosed vulnerabilities are documented in a human-readable format. Machine-readable formats are planned. A newsletter and an API are also planned but are not yet available.

[View the security information website](#)

Our release notes for the operating systems also carry information about fixes related to vulnerabilities:

[View the publications website](#)

Closing statements and further questions

Please direct any questions you may have to: security.rs-nc@rohde-schwarz.com ([OpenPGP](#))

Thank you for supporting a safer and more secure digital environment.

Wuerselen, October 8, 2026



Gregor Siegert
Lead IMT (Incident Management Team)

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions. 10/2026

ROHDE & SCHWARZ
Make ideas real

