VULNERABILITY DISCLOSURE POLICY

SPECS Surface Nano Analysis GmbH

SPECS Surface Nano Analysis GmbH ("SPECS") places great importance on the security of its products and welcomes cooperation with customers, partners, and security researchers in identifying and responsibly reporting security vulnerabilities.

This Vulnerability Disclosure Policy describes how vulnerabilities may be reported and how SPECS processes such reports.
If you have any questions regarding this document, please contact the SPECS Product Security Incident Response Team ("SPECS PSIRT") at psirt-spc@specs-group.com

Inquiries may be submitted in either German or English.

1 SCOPE

This Policy applies exclusively to the identification and reporting of security vulnerabilities in the following SPECS systems:

• All products and hardware systems placed on the market by SPECS (e.g., laser lithography
systems, maskless aligners, and nanofabrication equipment) within their official support
lifecycle, including their firmware-based control components.

• The IT infrastructure officially operated under the domain: https://specs-group.com/.

Explicitly Excluded (Out of Scope) from the legal protection provided by this Policy are:

• IT systems, cloud services, or software solutions of third parties, suppliers, or partners,
even where such systems interface with SPECS products.

• Physical security facilities of SPECS buildings and premises.

2 VULNERABILITY HANDLING PROCESS

All vulnerability reports are processed through the following steps:

2.1 REPORTING A VULNERABILITY

Security vulnerabilities in SPECS products, software, or components may be reported at any time to
the SPECS PSIRT:
E-Mail:

Telephone:
psirt-spc@specs-group.com
+49 30 467 824 0

To facilitate prompt handling of your report, please include the following information in your email:
• Reporter Name: If you wish to remain anonymous, we will respect your preference.
• Contact Details: E-mail address and telephone number where you can be reached.
• Affiliation: Please indicate your organization, if applicable.
• Type of Reported Vulnerability: Please describe the nature of vulnerability (e.g., network component, software, credentials, etc.).
• Trigger for the Vulnerability: Can you provide malicious code demonstrating the
vulnerability (Proof of Concept, PoC)? Alternatively, you may submit network traces (e.g.,
PCAP files) or a description of how the vulnerability may be triggered.
• Impact of the Vulnerability: Have you observed any effects caused by or resulting from the
vulnerability? Is this an actively exploited vulnerability?
• Affected Components: In which product, component, or software did you identify the
vulnerability? Please provide all available information, such as product family and group,
serial number, or software version.
• Confidentiality of the Vulnerability: Has the vulnerability already been disclosed, or do you
have specific plans for disclosure?

Privacy Notice
Personal data submitted as part of a vulnerability report (in particular name, contact details, and organizational affiliation) will be processed by SPECS solely for the purpose of handling the vulnerability report and communicating with the reporting individual, based on Article 6(1)(f) GDPR (legitimate interest in product security).

Further information regarding data processing, retention periods, and the rights of data subjects can be found in the SPECS Privacy Policy at: https://specs-group.com/data-protection/.

The SPECS PSIRT will acknowledge receipt of new vulnerability reports within two (2) business days.
Within a maximum of one (1) week after acknowledgement, the reporter will receive an initial substantive response regarding validation of the reported vulnerability. The SPECS PSIRT will provide regular status updates regarding processing progress, and in any event no less frequently than every two weeks.

The SPECS PSIRT thanks all reporters for their efforts to help improve the security posture of SPECS and its customers.

2.2 VALIDATION AND ANALYSIS OF VULNERABILITIES

During this phase, the SPECS PSIRT assesses the validity of the reported vulnerability. The relevance and applicability to SPECS products, components, software, and services are evaluated. In addition, SPECS assesses whether the vulnerability may potentially affect other customer systems, comparable product configurations, or third-party software and hardware components in use.
Additional information may be requested where necessary to verify and fully assess the report.
Where required by law, SPECS will comply with applicable reporting and notification obligations towards competent authorities, Computer Security Incident Response Teams (CSIRTs), and other relevant entities. This includes, in particular, mandatory reporting obligations under the European Cyber Resilience Act (CRA).

In the event of an actively exploited vulnerability or a serious security incident, SPECS will submit an early warning notification within 24 hours to the competent authority (in Germany, the Federal Office for Information Security (BSI)) and to ENISA. A full incident report including an initial assessment will follow within 72 hours, and a final report within 14 days (Article 14(3) and (4) CRA).

2.3 VULNERABILITY REMEDIATION AND DEVELOPMENT OF MITIGATION MEASURES

The SPECS PSIRT coordinates the handling of the reported vulnerability with the responsible
development and product expert teams to ensure a proper understanding of the issue and to develop appropriate remediation measures.
The impact on affected products, components, software solutions, as well as third-party and open source components in use, will be assessed. Based on this analysis, fixes, security updates, configuration changes, or other appropriate remediation measures will be developed, evaluated, and prioritized.

SPECS addresses vulnerabilities during the defined support period of the affected products and generally provides security updates free of charge through appropriate distribution mechanisms.
Where applicable, SPECS may provide the reporter with pre-release versions of fixes or mitigation measures to verify their effectiveness and support validation of the proposed solution.

2.4 PREPARATION AND PUBLICATION OF A SECURITY ADVISORY

In the final phase, the vulnerability is disclosed. Following successful validation of the effectiveness and compatibility of the fixes or mitigation measures, SPECS will prepare and publish a Security Advisory together with the corresponding patches, software updates, or recommended actions.
In the case of coordinated disclosure, the reporting individual or organization may, upon request, receive appropriate acknowledgment in the Security Advisory.

3 SAFE HARBOR

SPECS welcomes the responsible reporting of security vulnerabilities and will not initiate legal action against individuals who conduct security research in good faith and in compliance with the provisions of this Policy. Provided that you strictly comply with the terms of this Policy, SPECS hereby expressly authorizes access to the systems defined within the Scope solely for the purpose of security research. Such authorization constitutes authorized access and therefore excludes unauthorized access within the
meaning of Sections 202a et seq. of the German Criminal Code (Strafgesetzbuch, StGB). This

authorization applies only within the scope defined under "Scope" and subject to compliance with all other requirements of this Policy. Any activity exceeding such scope will not be protected.
Provided that you:
• investigate the vulnerability solely for the purposes of security research and reporting, and
do not circumvent barriers or protective mechanisms beyond what is necessary to verify
the vulnerability;
• respect the privacy, confidentiality, and availability of systems and data;
• do not modify, destroy, or disclose data;
• do not cause disruption to production, customer, or corporate systems;
• treat the vulnerability confidentially and do not publicly disclose it before SPECS has been
granted a period of at least ninety (90) days from receipt of a complete and reproducible
report to analyze and remediate the issue (Coordinated Disclosure), unless SPECS expressly
agrees in writing to an earlier disclosure;
• do not engage in social engineering, phishing, denial-of-service activities, or any other
activity that could impair the security, integrity, or availability of systems;
• immediately cease your investigation if you inadvertently gain access to personal,
confidential, or business-critical information,
SPECS will regard the reported activities as authorized security research and will not assert civil claims arising from the report or the associated research activities.

If at any time during your research you are uncertain whether a particular activity is permitted under this Policy, please contact the SPECS PSIRT before proceeding.

This Safe Harbor commitment applies exclusively to activities that:
1. are conducted in good faith;
2. comply with the provisions of this Policy; and
3. are intended to improve the security of SPECS products, components, software, or services.

SPECS reserves the right to exclude from this Safe Harbor any activities that violate applicable law, jeopardize personal data, disrupt business operations, or impair the availability of systems and services.

4 IV. GOVERNING LAW

This Policy and all legal issues arising out of or in connection with it shall be governed by the laws of Germany, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).