Novanta

Product Security

Report a Product Security Vulnerability

Policies and Procedures

Novanta is committed to the security of its products and services. We welcome good-faith reports from security researchers, customers, suppliers and others who believe they have identified a potential security vulnerability affecting a Novanta product or service.
This policy explains how to report a potential vulnerability, what information to provide, the conduct we ask reporters to follow, and what reporters can expect from Novanta. It is not a bug bounty program and does not promise payment or other compensation.

1 Scope

You may use this process to report a suspected product security vulnerability affecting:

- a Novanta product, including embedded software or firmware;
- a Novanta-provided software application, Software-as-a-Service (SaaS), digital service or remote data processing solution associated with a product; or
- a Novanta product security update.

The following products and activities are outside the scope of this process unless Novanta expressly states otherwise:

- third-party products or services that Novanta does not control;
- general product support, warranty or servicing requests;
- fraud, phishing, account-access or privacy complaints that do not concern a product security vulnerability; and
- denial-of-service testing, social engineering, physical intrusion or testing that could affect safety, production, clinical, industrial or other live operations.

For urgent safety concerns, suspected active exploitation or an ongoing security incident, clearly mark the report "URGENT" and explain the immediate risk.

2 How to Report

Please submit reports through one of the following channels:

Type	Details
Email	ProductSecurityReport@novanta.com
Form	https://novanta.com/product-security/#report

Please do not send sensitive personal data, confidential patient/customer information, production data, credentials or exploit code by unencrypted email. If sensitive material is necessary to validate the report, first ask Novanta to provide an approved secure transfer method, and obtain appropriate data release consent from all relevant parties.

3 What to Include

A report should include, where available:

- the affected product, model, software or firmware version;
- product deployment (e.g.: standalone, OEM, etc.)
- a clear description of the suspected vulnerability and its potential impact (proof-of-concept material, logs or screenshots, with sensitive information removed);
- the (testing) environment and tools used;
- any known mitigations or suggested remediation;
- whether you have reported the issue to any other party; and
- your name and a reliable contact method, unless you choose to report anonymously.

Please submit one vulnerability per report where practicable. If several findings appear related, explain the relationship between them.

4 Responsible Research Guidelines

To support safe and coordinated handling, please:

- comply with applicable law and test only assets you own or are expressly authorized to test;
- avoid testing products or systems that are actively used in safety-critical, clinical, industrial, production or customer environments;
- avoid accessing, copying, retaining, changing or deleting data beyond the minimum necessary to demonstrate the issue;
- stop testing and notify Novanta promptly if you encounter personal data, confidential information, safety risks, service disruption or evidence of active exploitation;
- do not use social engineering, phishing, physical intrusion, denial-of-service, brute-force or destructive techniques;
- do not install persistence, backdoors, malware or additional code unrelated to demonstrating the issue;
- do not use the vulnerability to obtain a commercial advantage, demand payment or threaten disclosure; and
- give Novanta a reasonable opportunity to investigate and address the issue before public disclosure and coordinate proposed disclosure timing with Novanta.

This policy does not grant access to any product, system, premises, data or account, and does not waive any applicable rights. Novanta cannot authorize conduct on systems or products owned or controlled by third parties.

5 Our Response

After receiving a report, Novanta intends to:

- acknowledge receipt;
- assign a reference number or other tracking identifier where appropriate;
- review the report and request additional information if needed;
- coordinate internally and, where relevant, with affected suppliers, customers, vulnerability coordinators or other third parties;
- provide status updates at appropriate intervals, subject to the sensitivity and complexity of the issue; and
- inform the reporter when the matter is closed or when a remediation or other response is available, where appropriate.

Note that in the case of anonymous reports, Novanta may not be able to acknowledge or provide status and closure updates to the reporter.

Investigation and remediation timeframes depend on factors such as the affected product, exploitability, safety implications, availability of fixes, required validation and coordination with third parties. Unless expressly agreed in writing, this policy does not create a commitment to remediate or disclose a reported issue within a fixed period.

6 Coordinated Disclosure and Recognition

Please do not publicly disclose the vulnerability or related technical details until Novanta has had a reasonable opportunity to investigate and, where appropriate, make a remediation available. Novanta will seek to discuss disclosure timing in good faith, taking account of the risk to users and the public, the availability of mitigations, third-party dependencies and any legal obligations.

Novanta does not currently operate a public researcher recognition program.

7 Confidentiality and Personal Data

Novanta will use information submitted through this process to assess, investigate and respond to the report, protect products and users, comply with legal obligations, and improve security. Novanta may share relevant information with affiliated companies, service providers, suppliers, customers, vulnerability

coordinators or authorities where reasonably necessary for those purposes, subject to appropriate safeguards and legal requirements.

For information about Novanta's handling of personal data, see https://novanta.com/privacy-policy/. Do not include personal data that is not necessary for the report.

8 Changes and Contact

Novanta may update this policy to reflect changes in its products, processes, or legal requirements. The version published at https://novanta.com/product-security/#cvd is the current version.

Questions about this policy may be sent to ProductSecuritySupport@novanta.com.