Responsible Disclosure Program

Northvolt is committed to maintaining the security of our systems and our customers' information. We appreciate and encourage security researchers to contact us to report potential vulnerabilities identified in any product, system, or asset belonging to Northvolt.

If you believe you have identified a potential security vulnerability, please share it with us by following the submission guidelines below. Thank you in advance for your submission, we appreciate researchers assisting us in our security efforts.

Responsible Disclosure Program Guidelines

Researchers shall disclose potential vulnerabilities to Northvolt in accordance with the following guidelines:

1 Do not engage in any activity that can potentially or actually cause harm to Northvolt, our customers, or our employees.
2 Do not engage in any activity that can potentially or actually stop or degrade Northvolt services or assets.
3 Do not engage in any activity that violates (a) local laws or regulations or (b) the laws or regulations of any country where (i) data, assets or systems reside, (ii) data traffic is routed or (iii) the researcher is conducting research activity.
4 Do not store, share, compromise or destroy Northvolt or customer data. If Personally Identifiable Information (PII) is encountered, you should immediately halt your activity, purge related data from your system, and immediately contact Northvolt. This step protects any potentially vulnerable data, and you.
5 Do not initiate a fraudulent financial transaction.
6 Provide Northvolt AB reasonable time to fix any reported issue, before such information is shared with a third party or disclosed publicly.

By responsibly submitting your findings to Northvolt in accordance with these guidelines Northvolt agrees not to pursue legal action against you. Northvolt reserves all legal rights in the event of noncompliance with these guidelines.

Once a report is submitted, Northvolt commits to provide prompt acknowledgement of receipt of all reports (within two to three business days of submission) and will keep you reasonably informed of the status of any validated vulnerability that you report through this program.

Out of Scope Vulnerabilities

Certain vulnerabilities are considered out of scope for our Responsible Disclosure Program. Out-of-scope vulnerabilities include:

- Physical Testing
- Social Engineering. For example, attempts to steal cookies, fake login pages to collect credentials
- Phishing
- Denial of service attacks
- Resource Exhaustion Attacks

Submission Format

When reporting a potential vulnerability, please include a detailed summary of the vulnerability, including the target, steps, tools, and artifacts used during discovery (screen captures welcome).

Submission Instructions

Please submit your report via email to the following email address:

responsibledisclosure@northvolt.com