2025-02-13

Vulnerability Disclosure Policy

NIBE Group is committed to safeguarding and protecting our customers, our information and any other information entrusted to us.

This means we take cyber security issues very seriously and recognize the importance of privacy, security, and community outreach. As such, we are committed to addressing and reporting security issues through a coordinated and constructive approach; designed to drive the greatest protection for technology users and protection of information relating to our company, customers, consumers, and employees.

When properly notified of legitimate issues, we will do our best to acknowledge your vulnerability report, assign resources to investigate the issue and solve potential problems as quickly as possible. Whether you are a user of NIBE Group products, a software developer or simply a security enthusiast, you are an important part of this process.

Reporting Security Issues

A Vulnerability is a weakness or flaw in an IT-system, network or process that can be exploited by a threat actor to gain unauthorized access to data or system resources. Vulnerabilities can arise from various factors, such as software bugs, misconfigurations, or human errors.

If you believe you have discovered a vulnerability in a NIBE Group asset / system or have a security incident to report, please send an email to vulnerability@nibegroup.com. Vulnerabilities shall be reported as soon as possible, but preferably no later than 24 hours after you have discovered it.

In all cases, you must:

- Respect our privacy. Contact us immediately if you access anyone else's data, personal or of any other kind. This includes usernames, passwords and other credentials. You must not save, store or transmit this information.
- Act in good faith. You should report the vulnerability to us honestly with no conditions attached.
- Work with us. Promptly report any findings to us, stop after you find the first vulnerability and request permission to continue testing. Allow us a reasonable amount of time to resolve the vulnerability, and contact us, well before publicly disclosing it.

And you must not:

- Exfiltrate data. Instead use a proof of concept to demonstrate a vulnerability.
- Exploit a vulnerability to disable further security controls.
- Perform social engineering.
- Use automated scanners.

Please note that there is a separate procedure for reporting incidents that include personal data (personal data breaches). For more information, see NIBE's Privacy Policy.

Post-Report Process

Upon receipt of a vulnerability / security report, NIBE will undertake a series of steps to address the issue:

1. NIBE Group requests the reporter to keep any communication regarding the vulnerability confidential.
2. NIBE Group investigates and verifies the vulnerability.
3. NIBE Group addresses the vulnerability and releases an update or patch to the software. If for some reason this cannot be done quickly or at all, NIBE will provide information on recommended mitigations.
4. NIBE Group will keep the reporter informed of the progress with an initial acknowledgment within 5 business days of receipt and with an aim to provide subsequent status updates on a monthly basis.
5. After a resolution has been published, NIBE Group will determine whether the vulnerability reporter is entitled to receive a reward or bounty for the finding.

We greatly appreciate the efforts of security researchers and discoverers who share information on security issues with us, giving us a chance to improve our products and services and better protect our customers. Thank you for working with us through the above process.

Approved by the Board of NIBE Industrier AB 2025-02-13