Product cyber security

Responsible disclosure policy

12 March 2024
Version 1.0

LIEBHERR

Liebherr-International AG

Introduction

At Liebherr, we acknowledge the valuable role that security researchers, partners, customers, and other parties play in identifying and addressing potential security issues in our products. This responsible disclosure policy outlines the guidelines and our commitment for reporting security issues for Liebherr products. Liebherr's Product Security Incident Response Team (PSIRT) receives all submitted security issues, coordinates the communication on both sides internal and external, and makes sure that security updates are issued.

Scope

This policy covers all Liebherr products both hardware and software. If you believe you have discovered a security issue, please report it to us following the guidelines outlined in this document.

Not in scope

The following topics are not covered by this policy:

- Security issues in Liebherr's IT systems, like the Liebherr website etc.
- Customer support requests
- Products having reached end-of-life
- Duplicate vulnerability reports, e.g., when other researchers having reported the identical vulnerability earlier, or previously published vulnerabilities

Responsible disclosure guidelines

- **Report security issues promptly:** We encourage security researchers to promptly report any discovered security issues to Liebherr using the provided contact form.
- **Provide adequate information:** We ask you to include as much information as possible to help our team understand and replicate the issue. This may include screenshots, code snippets, or other relevant details.
- **Responsible testing:** Only test security issues on your own accounts, your own machines, or on accounts/devices for which you have explicit permission to do so. Unauthorized access to, or disruption of our systems or data is strictly prohibited.
- **Confidentiality:** Keep the security issue details confidential until Liebherr has had a reasonable opportunity to address the issue. Do not disclose the security issue publicly or to any third-party without our explicit consent.

Our commitment

- **Non-retaliation:** Liebherr does not take legal action against security researchers who responsibly disclose security issues when adhering to the guidelines outlined in this policy.
- **Resolution:** Our team is committed to investigate and resolve reported security issues. We will inform the sender on the status of the resolution process.
- **Anonymity:** We respect the anonymity of the reporting party and allow to submit security issues without you having to disclose your real name.

Process

1. **Report:** One submits a potential security issue via Liebherr's contact form. We will acknowledge the receipt of the report within two business days.
2. **Analysis:** Liebherr's PSIRT takes care of the potential security issue and gets in contact with the internal product development team to analyse the validity and reproduce the potential security issue. We may come back to the sender of the potential security issue to provide further information.
3. **Handling:** If the validity of the security issue is confirmed, the PSIRT will coordinate the mitigation handling. If applicable, Liebherr will provide mitigation information or security updates to the relevant parties.
4. **Disclosure:** Liebherr will inform the sender and relevant parties of confirmed vulnerabilities including countermeasures.

Contact

For reporting security issues or seeking clarification on any aspect of this policy, please contact the PSIRT via the contact form. Liebherr appreciates the cooperation with the security community to help us continuously improve Liebherr's product security. Feel free to submit your security issues in English or German.

Company address

Liebherr-International AG • Rue Hans-Liebherr 7 • 1630 Bulle • Switzerland • liebherr.com