Hilti Vulnerability Disclosure Policy

Valid as of 01.01.2026

DOCUMENT CONTROL

Change History

Version	Release date	Author	Summary of changes	Approved by
1.0	01.01.2026	Philipp Blaas	▪ Initial enactment	Thomas Rhomberg, CCSO

Table 1: Change History

1 INTRODUCTION

At Hilti, our mission to make construction better extends to the digital realm. We recognize that the security of our products and services is fundamental to the trust that our customers place in us by using our offerings. To uphold this trust, we actively welcome and value contributions from the security researcher community. We appreciate the efforts made by any individual reporting vulnerabilities or errors within our websites, products or services.

2 REPORTING A VULNERABILITY

To report a vulnerability, please use the secure contact information on this page for submitting reports to ensure secure transmission and timely processing. Reports should be submitted in English or German to facilitate efficient handling.

3 HILTI COMMITMENT

Hilti takes all vulnerability reports seriously and commits to:

- Acknowledge receipt of your report promptly.
- Ensure that your report is processed without undue delay
- Where feasible, provide an estimate for remediation or mitigation.
- Use your contact details solely for the purpose of clarifying your report or updating you on its status.

Hilti will not pursue legal action or claims against you for security research activities and reports submitted in good faith under this policy, provided that you have complied with applicable law and the terms of this policy at all times.

4 YOUR COMMITMENT

To comply with this policy, you must:

- Not cause any harm to Hilti, our customers, or others.
- Not compromise the privacy or safety of our customers, employees or the operation of our products or services.
- Not exploit or use in any manner (other than for the purpose of reporting to Hilti), the discovered vulnerabilities.
- Not violate any applicable law or regulation.
- Not publicize details about any vulnerability unless Hilti has confirmed completed remediation of the vulnerability.
- Not conduct social engineering, spamming, phishing, denial-of-service or resource-exhaustion attacks.
- Not test the physical security of any property, building, plant or factory of Hilti.
- Agree that you are making your report without any expectation or requirement of reward or other benefit, financial or otherwise.
- Not access unnecessary, excessive or significant amounts of data.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).