VULNERABILITY DISCLOSURE POLICY FOR THE EINHELL CONNECT APP AND RELATED IOT DEVICES

Einhell Germany AG (hereinafter referred to as „the company“) is committed to addressing and reporting security issues through a coordinated and constructive approach designed to provide the greatest protection for the company‘s customers, partners, staff, and all Internet users.

A security vulnerability is a weakness in our systems or services that may compromise their security. This policy applies to security vulnerabilities discovered by both the company staff and by others, using the company‘s service Einhell Connect App in relation to the supported IoT devices.

Vulnerability Monitoring used for Einhell Connect App:

- Support service: Collecting of user feedback and using of an internal ticketing portal to notify relevant managers/operators
- Development framework – nuget.org service: An automated vulnerability scan and notification is used for connected software
- st.com PSIRT notifications monitoring for firmware-related software updates and vulnerability notifications
- Regular peer review and code review
- Irregular automated code analysis

Reporting vulnerabilities:

If you believe to have discovered a vulnerability in one of our services or have a security incident to report, please send an E-mail to security-connect@einhell.com.

Please use the following categorization when reporting vulnerabilities:

- **Critical vulnerabilities**, including those that can lead to unauthorized access, data breaches, remote code execution, or system compromise, should be reported immediately upon discovery
- **High severity vulnerabilities**, including issues that pose a significant security risk but may not result in immediate compromise, should be reported within 30 days of discovery

Depending on the type of vulnerability, we will try to provide a solution within the timeline below. Please be aware that we reserve the right to postpone the deadline if it ends on a weekend (Saturday/Sunday) or a public holiday. In this case, the deadline will be postponed to the next regular working day.

- Mobile application, Device firmware, APIs, Web interface and Cloud infrastructure: We commit to fixing identified vulnerabilities in this category within 90 days from the date of disclosure.
- Hardware: If changes to the hardware are required, these will be implemented with the next production batch following the disclosure of the vulnerability. The specific timeline for implementation will be communicated to the reporter during the coordination and resolution process.

Once we have received a vulnerability report, the company takes a series of steps to address the issue:

- We will provide acknowledgement of receipt of your report within 5 working days
- We request the reporter to keep any communication regarding the vulnerability confidential
- We will work with you to understand and investigate the vulnerability
- We will quickly provide a planned timeframe for the investigation and a proposed fix
- We will notify you once the vulnerability has been resolved, to allow retesting by the reporter if needed
- We publicly announce the vulnerability in the release notes of the update. We may also issue additional public announcements, for example via social media
- Release notes or other social media posts may include a reference to the person/people who reported the vulnerability unless the reporter(s) would prefer to stay anonymous

The company will try to keep the reporter apprised of steps in this process. You will receive an update on the reported issue every two weeks until the solution is published.

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 services, and better protect our customers. We take the confidentiality of vulnerability reports seriously and will handle all reports and related communication with the reporter in a confidential manner. We request that the reporter keep any communication regarding the vulnerability confidential until we have had a chance to investigate and resolve the issue. We will work with the reporter to determine an appropriate level of disclosure once the vulnerability has been resolved. In line with general responsible disclosure good practice, we ask that security researchers:

- Provide sufficient detail about the vulnerability to allow us to investigate successfully including steps required to reproduce the issue
- We appreciate the use of the Common Vulnerability Scoring System when reporting a vulnerability
- Do not modify or delete data, or take actions that would impact on the company's customers
- Do not carry out social engineering exercises or attempt to find weaknesses in the physical security of company offices or other locations

This Vulnerability Disclosure Policy is subject to change without notice. The policy is not a contract and does not create any legal obligations or liabilities for Einhell Germany AG. The company reserves the right to update the policy as necessary to reflect changes in its products, services, or business practices. By submitting a vulnerability report, you agree to abide by the terms and conditions of this policy and any updates or revisions. If you have any questions or concerns about the policy, please contact security-connect@einhell.com.

We appreciate your cooperation in helping us maintain the security of our products and services.