Hugo Brennenstuhl GmbH & Co KG - Seestr. 1-3 - 72074 Tübingen

Policy for the disclosure of product-related cybersecurity vulnerabilities

1. Introduction

This policy of **Hugo Brennenstuhl GmbH & Co. Kommanditgesellschaft** defines the procedures and expectations for the detection, reporting and remediation of vulnerabilities in our products in accordance with the EN 303 645 standard (CYBER - Cybersecurity in the consumer area of the Internet of Things). It applies to all employees, partners and external security researchers who interact with our systems.

2. Purpose

The purpose of this policy is:

- To ensure the safety and integrity of our products.
- Promote collaboration with the security research community.
- Provide a clear and structured process for reporting and resolving vulnerabilities.

3. Definitions

- **Vulnerability**: An error or weakness in a system that can be exploited to allow unauthorized access or other negative effects.
- **Security researcher**: A person who identifies and reports vulnerabilities in systems in order to improve their security.
- **Reporting party**: The person or organization that discovers and reports a vulnerability.

4. Process for reporting vulnerabilities

4.1 Vulnerability report

- Vulnerabilities can be reported via our online reporting form.
- The message should contain the following information:
    - A description of the vulnerability.
    - The products or services concerned.
    - Steps to reproduce the vulnerability.
    - Contact information of the reporting party for queries.

Date	Created / Changed	Version	Affected chapters	Reason for the change(s)	Release GL:
19.07.2024	Wob	1	all	-	SB

4.2 Confirmation of receipt

- Our security team will confirm receipt of the report within 7 working days of receipt.
- The notifier is assigned a case number that is used for further communication.

4.3 Investigation and validation

- Our security team investigates and validates the reported vulnerability.
- If additional information is required, the security team will contact the reporter.

4.4 Remediation and communication

- After validation, a plan is drawn up to rectify the vulnerability.
- The reporting party is informed about the progress of the rectification.
- Once the rectification has been completed, the reporting party is informed of the measures taken.

5. Publication and disclosure

- Once the vulnerability has been rectified, public disclosure can be made in consultation with the reporting party.
- The disclosure does not contain any information that could be used to exploit the vulnerability before a fix is available.

6 Confidentiality and data protection

- All information about reported vulnerabilities is treated confidentially.
- Personal data of the reporting party will be processed and protected in accordance with the applicable data protection regulations.

7 Responsibilities

- The security team is responsible for investigating and remedying reported vulnerabilities.
- The management supports the security team in providing the necessary resources to eliminate the vulnerabilities.

Date	Created / Changed	Version	Affected chapters	Reason for the change(s)	Release GL:
19.07.2024	Wob	1	all	-	SB

8. Guidelines on disclosure

8.1 Coordination and cooperation

- We work closely with other affected parties, including suppliers and, where appropriate, third parties, to effectively address vulnerabilities.
- Joint disclosures are coordinated to ensure the security of the entire supply chain.

8.2 Timetable for disclosure

- A coordinated disclosure will only be made when a fix or security update is available.
- We aim to rectify vulnerabilities within 90 days of notification. In cases where more time is required, the reporting party will be informed accordingly.

8.3 Emergency measures

- In the case of critical vulnerabilities that require immediate action, a temporary fix or workaround is provided immediately.

9. Support period for security updates

- Security updates are provided for a period of at least 2 years after purchase of a product if required.

10. Continuous improvement

- This policy is regularly reviewed and updated to ensure that it reflects current threats and best practice.
- Feedback and suggestions for improvement are taken into account in order to increase the effectiveness of the policy.

By implementing this policy, our company ensures that vulnerabilities are dealt with effectively and promptly in order to continuously improve the security of our products.

The management

Date	Created / Changed	Version	Affected chapters	Reason for the change(s)	Release GL:
19.07.2024	Wob	1	all	-	SB