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

Politik zur Offenlegung von produktbezogenen Cybersecurity Schwachstellen

1. Einführung

Diese Politik der **Hugo Brennenstuhl GmbH & Co. Kommanditgesellschaft** definiert die Verfahren und Erwartungen für die Entdeckung, Meldung und Behebung von Schwachstellen in unseren Produkten gemäß der Norm EN 303 645 (CYBER - Cybersecurity im Konsumenten-Bereich des Internets der Dinge). Sie gilt für alle Mitarbeiter, Partner und externe Sicherheitsforscher, die mit unseren Systemen interagieren.

2. Zweck

Der Zweck dieser Politik ist es:

- Die Sicherheit und Integrität unserer Produkte zu gewährleisten.
- Die Zusammenarbeit mit der Sicherheitsforschergemeinschaft zu fördern.
- Einen klaren und strukturierten Prozess zur Meldung und Behebung von Schwachstellen zu bereitzustellen.

3. Definitionen

- **Schwachstelle**: Ein Fehler oder eine Schwäche in einem System, die ausgenutzt werden kann, um unbefugten Zugriff oder andere negative Auswirkungen zu ermöglichen.
- **Sicherheitsforscher**: Eine Person, die Schwachstellen in Systemen identifiziert und meldet, um deren Sicherheit zu verbessern.
- **Meldender**: Die Person oder Organisation, die eine Schwachstelle entdeckt und meldet.

4. Prozess zur Meldung von Schwachstellen

4.1 Schwachstellenmeldung

- Schwachstellen können über unser Online-Meldeformular gemeldet werden.
- Die Meldung sollte folgende Informationen enthalten:
  - Eine Beschreibung der Schwachstelle.
  - Die betroffenen Produkte oder Dienste.
  - Schritte zur Reproduktion der Schwachstelle.
  - Kontaktinformationen des Meldenden für Rückfragen.

Datum	Erstellt / Geändert	Version	Betroffene Kapitel	Grund der Änderung(en)	Freigabe GL:
19.07.2024	Wob	1	alle	-	SB

4.2 Bestätigung des Eingangs

- Innerhalb von 7 Werktagen nach Eingang der Meldung bestätigt unser Sicherheitsteam den Erhalt der Meldung.
- Dem Meldenden wird eine Fallnummer zugewiesen, die für die weitere Kommunikation verwendet wird.

4.3 Untersuchung und Validierung

- Unser Sicherheitsteam untersucht und validiert die gemeldete Schwachstelle.
- Wenn zusätzliche Informationen benötigt werden, wird das Sicherheitsteam den Meldenden kontaktieren.

4.4 Behebung und Kommunikation

- Nach der Validierung wird ein Plan zur Behebung der Schwachstelle erstellt.
- Der Meldende wird über den Fortschritt der Behebung informiert.
- Nach Abschluss der Behebung wird der Meldende über die durchgeführten Maßnahmen informiert.

5. Veröffentlichung und Offenlegung

- Wenn die Schwachstelle behoben ist, kann eine öffentliche Offenlegung in Absprache mit dem Meldenden erfolgen.
- Die Offenlegung enthält keine Informationen, die zur Ausnutzung der Schwachstelle verwendet werden könnten, bevor ein Fix verfügbar ist.

6. Vertraulichkeit und Datenschutz

- Alle Informationen über gemeldete Schwachstellen werden vertraulich behandelt.
- Personenbezogene Daten des Meldenden werden gemäß den geltenden Datenschutzbestimmungen verarbeitet und geschützt.

7. Verantwortlichkeiten

- Das Sicherheitsteam ist verantwortlich für die Untersuchung und Behebung gemeldeter Schwachstellen.
- Die Geschäftsleitung unterstützt das Sicherheitsteam bei der Bereitstellung der notwendigen Ressourcen zur Behebung der Schwachstellen.

Datum	Erstellt / Geändert	Version	Betroffene Kapitel	Grund der Änderung(en)	Freigabe GL:
19.07.2024	Wob	1	alle	-	SB

8. Richtlinien zur Offenlegung

8.1 Koordination und Zusammenarbeit

- Wir arbeiten eng mit anderen betroffenen Parteien, einschließlich Lieferanten und ggf. Drittanbietern, zusammen, um Schwachstellen effektiv zu beheben.
- Gemeinsame Offenlegungen werden koordiniert, um die Sicherheit der gesamten Lieferkette zu gewährleisten.

8.2 Zeitplan für die Offenlegung

- Eine koordinierte Offenlegung wird erst vorgenommen, wenn ein Fix oder ein Sicherheitsupdate verfügbar ist.
- Wir streben an, Schwachstellen innerhalb von 90 Tagen nach Meldung zu beheben. In Fällen, in denen mehr Zeit erforderlich ist, wird der Meldende entsprechend informiert.

8.3 Notfallmaßnahmen

- Bei kritischen Schwachstellen, die sofortige Maßnahmen erfordern, wird umgehend ein temporärer Fix oder ein Workaround bereitgestellt.

9. Unterstützungszeitraum für Sicherheitsupdates

- Sicherheitsupdates werden für einen Zeitraum von mindestens 2 Jahren nach Kauf eines Produktes bereitgestellt sofern erforderlich.

10. Kontinuierliche Verbesserung

- Diese Politik wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie aktuellen Bedrohungen und bewährten Verfahren entspricht.
- Rückmeldungen und Verbesserungsvorschläge werden berücksichtigt, um die Effektivität der Politik zu steigern.

Durch die Umsetzung dieser Politik stellt unser Unternehmen sicher, dass Schwachstellen effektiv und zeitnah behandelt werden, um die Sicherheit unserer Produkte kontinuierlich zu verbessern.

Die Geschäftsleitung

Datum	Erstellt / Geändert	Version	Betroffene Kapitel	Grund der Änderung(en)	Freigabe GL:
19.07.2024	Wob	1	alle	-	SB