RICHTLINIE ZUR BEKANNTGABE VON SICHERHEITSRISIKEN (VDP) FÜR DIE EINHELL CONNECT APP UND ZUGEHÖRIGE IOT-GERÄTE

Die Einhell Germany AG (im Folgenden als „das Unternehmen“ bezeichnet) verpflichtet sich, Sicherheitsrisiken durch einen koordinierten und konstruktiven Ansatz anzugehen und zu melden, um den größtmöglichen Schutz für die Kunden, Partner und Mitarbeiter des Unternehmens sowie alle Internetnutzer zu gewährleisten.

Ein Sicherheitsrisiko ist eine Schwachstelle in unseren Systemen oder Diensten, die deren Sicherheit gefährden kann. Diese Richtlinie gilt für Sicherheitsrisiken, die sowohl von Mitarbeitern des Unternehmens als auch anderen Personen entdeckt werden, die die Einhell Connect App im Zusammenhang mit den unterstützten IoT-Geräten verwenden.

Vulnerability Monitoring der Einhell Connect App:

- Support Service: Sammeln von Kundenfeedback und Nutzung eines internen Ticketing-Portals zur Benachrichtigung der zuständigen Manager/Mitarbeiter
- Entwicklungsframework – nuget.org Service: Automatischer Schwachstellen-Scan mit Benachrichtigungsservice wird für die verbundene Software verwendet
- PSIRT-Benachrichtigungen von st.com: Überwachung von Firmware-bezogenen Software-Updates und Benachrichtigungen über Sicherheitslücken
- Regelmäßige Peer-Review und Code-Review
- Unregelmäßige automatische Code-Analyse

Meldung von Sicherheitsschwachstellen:

Wenn Sie glauben, eine Schwachstelle in einem unserer Dienste entdeckt zu haben oder einen Sicherheitsvorfall zu melden haben, senden Sie bitte eine E-Mail an security-connect@einhell.com.

Bitte verwenden Sie folgende Einstufung beim Melden von Sicherheitsrisiken:

- **Kritische Schwachstelle**, einschließlich solcher, die zu unbefugtem Zugriff, Datenverletzungen, Remotecodeausführung oder System-Kompromittierung führen können, sollten sofort nach Entdeckung gemeldet werden
- **Schwachstelle mit hohem Schweregrad**, einschließlich solcher, die ein erhebliches Sicherheitsrisiko darstellen, aber nicht zu einer unmittelbaren Gefährdung führen, sollten innerhalb von 30 Tagen nach ihrer Entdeckung gemeldet werden

Je nach Art des Sicherheitsrisikos werden wir versuchen, innerhalb des angegebenen Zeitrahmens eine Lösung anzubieten. Bitte beachten Sie, dass wir uns das Recht vorbehalten, die Frist zu verschieben, wenn sie auf ein

Wochenende (Samstag/Sonntag) oder einen Feiertag fällt. In diesem Fall wird die Frist auf den nächsten regulären Arbeitstag verschoben.

- Mobile Anwendung, Geräte-Firmware, APIs, Web-Schnittstelle und Cloud-Infrastruktur:
  Wir verpflichten uns identifizierte Schwachstellen in dieser Kategorie innerhalb von 90 Tagen ab dem Datum der Offenlegung zu beheben

- Hardware: Wenn Änderungen an der Hardware erforderlich sind, werden diese mit der nächsten Produktionscharge nach dem Bekanntwerden der Schwachstelle umgesetzt. Der genaue Zeitplan der Umsetzung wird dem Meldenden während des Koordinierungs- und Lösungsprozesses mitgeteilt

Sobald wir eine Meldung über eine Sicherheitslücke erhalten haben, unternimmt das Unternehmen eine Reihe von Schritten, um das Problem zu beheben:

- Wir bestätigen den Eingang Ihrer Meldung innerhalb von 5 Arbeitstagen

- Wir bitten den Meldenden, jegliche Kommunikation über die Sicherheitslücke vertraulich zu behandeln

- Wir werden mit Ihnen zusammenarbeiten, um die Schwachstelle zu verstehen und zu untersuchen

- Wir benachrichtigen Sie schnellstmöglich über den geplanten Zeitrahmen der Prüfung und einen Vorschlag zur Behebung der Schwachstelle

- Wir benachrichtigen Sie, sobald die Schwachstelle behoben ist, damit der Meldende sie bei Bedarf erneut testen kann

- Wir geben die Sicherheitslücke in den Versionshinweisen des Updates öffentlich bekannt. Wir könnten außerdem weitere öffentliche Bekanntmachungen herausgeben, zum Beispiel über soziale Medien

- In den Versionshinweisen oder anderen Beiträgen in sozialen Medien kann ein Verweis auf Person(en) enthalten sein, die die Sicherheitslücke gemeldet hat/haben, es sei denn, der/die Meldende(n) möchte(n) lieber anonym bleiben

Das Unternehmen wird sich bemühen, den Meldenden über die einzelnen Schritte in diesem Prozess auf dem Laufenden zu halten.

Wir schätzen die Bemühungen von Sicherheitsexperten und -prüfern sehr, die uns Informationen über Sicherheitsprobleme mitteilen und uns so die Möglichkeit geben, unsere Dienste zu verbessern und unsere Kunden besser zu schützen. Wir nehmen die Vertraulichkeit von Meldungen über Sicherheitslücken ernst und behandeln alle Meldungen und die damit verbundene Kommunikation mit dem Meldenden vertraulich. Wir bitten den Meldenden, jegliche Kommunikation über die Sicherheitslücke vertraulich zu behandeln, bis wir die Möglichkeit hatten, das Problem zu untersuchen und zu lösen. Sobald die Schwachstelle behoben ist, werden wir gemeinsam mit dem Meldenden einen angemessenen Grad der Offenlegung festlegen. Im Einklang mit der allgemeinen guten Praxis der verantwortungsvollen Offenlegung bitten wir Sicherheitsforscher:

- Geben Sie genügend Details über die Schwachstelle an, einschließlich der Schritte, die erforderlich sind, um das Problem zu reproduzieren

- Wir begrüßen die Verwendung des Common Vulnerability Scoring System bei der Meldung einer Sicherheitslücke

- Ändern oder löschen Sie keine Daten und führen Sie keine Maßnahmen durch, die sich auf die Kunden des Unternehmens auswirken würden

- Führen Sie keine Social-Engineering-Übungen durch und versuchen Sie nicht, Schwachstellen in der physischen Sicherheit von Firmenbüros oder anderen Standorten zu finden

Diese Richtlinie kann ohne vorherige Ankündigung geändert werden. Die Richtlinie stellt keinen Vertrag dar und begründet keine rechtlichen Verpflichtungen oder Haftungen für die Einhell Germany AG. Das Unternehmen behält sich das Recht vor, diese Richtlinie bei Bedarf zu aktualisieren, um Änderungen an seinen Produkten, Dienstleistungen oder Geschäftspraktiken zu berücksichtigen. Durch das Einreichen eines Schwachstellenberichts erklären Sie sich damit einverstanden, sich an die Bedingungen dieser Richtlinie und alle Aktualisierungen oder Überarbeitungen zu halten. Wenn Sie Fragen oder Bedenken zu dieser Richtlinie haben, wenden Sie sich bitte an securityconnect@einhell.com.

Wir schätzen Ihre Mitarbeit bei der Aufrechterhaltung der Sicherheit unserer Produkte und Dienstleistungen.