SICK AG Vulnerability Handling Guideline

Das SICK PSIRT begrüßt Schwachstellenmeldungen von jedem, unabhängig von einem etwaigen Kundenstatus und untersucht diese gewissenhaft. Zu den Berichterstattern zählen unter anderem Sicherheitsforscher, Hochschulen, CERTs, Geschäftspartner, Behörden, Industrieverbände und Lieferanten. Das Aufdecken von Schwachstellen wird als ein gemeinsames Bestreben verschiedenster Parteien verstanden, mit dem Ziel unseren Kunden durchgängig ein hohes Sicherheitsniveau zu bieten. Dies ist insbesondere bedeutend, da Produkte der SICK AG wichtige Schutzfunktionen erfüllen und in kritischen Infrastrukturen eingesetzt werden. Um alle Parteien in einer koordinierten Schwachstellenmeldung zu bestärken, wird der Prozess transparent in diesem Dokument beschrieben.

Während des gesamten Ablaufs ist das SICK PSIRT darin bestrebt, vertrauensvoll und professionell mit allen Beteiligten zusammenzuarbeiten. Bei Fragen zu diesem Dokument gibt das SICK PSIRT unter psirt@sick.de Auskunft. Ein Kontakt kann in den Sprachen Deutsch oder Englisch erfolgen.

Die Schritte des Prozesses sind:

Bericht

Eine Schwachstelle wird an das SICK PSIRT gemeldet. Informationen zur Kontaktmöglichkeit und dem Inhalt einer Meldung sind unter https://www.sick.com/psirt aufgeführt. Für eine Zusammenarbeit ist weder eine Geheimhaltungsvereinbarung (NDA) noch ein anderer Vertrag notwendig oder Voraussetzung.

Analyse

Das SICK PSIRT überprüft alle eingehenden Meldungen formal auf Vollständigkeit und Relevanz. Anschließend werden diese an die entsprechenden Entwicklungsbereiche weitergeleitet und untersucht. Bei Bedarf werden Partner, oder andere CERTs informiert und in den Vorgang eingebunden. Es erfolgt eine regelmäßige Kommunikation mit dem Berichterstatter.

Lösung

Die produktverantwortlichen Bereiche entwickeln eine Lösung, um das Risiko der Schwachstelle angemessen zu behandeln. Das SICK PSIRT unterstützt und koordiniert die Aktivitäten. Falls es vom Berichterstatter gewünscht und technisch möglich ist, kann die Wirksamkeit einer Lösung gemeinsam überprüft werden.

Offenlegung

Im finalen Schritt wird die Schwachstelle zu einem abgestimmten Zeitpunkt veröffentlicht. In einem Sicherheits-Advisory werden eine Beschreibung der Schwachstelle und erforderliche Maßnahmen zur Beseitigung aufgeführt. Wenn dem Prozess einer koordinierten Offenlegung der Schwachstelle gefolgt wurde, kann der Berichterstatter öffentlich anerkannt werden.