Informationen zur CyberSecurity

Umgang mit Schwachstellen bei MEIKO

Einleitung

MEIKO ist dankbar für alle Hinweise zu Sicherheitsrisiken und bearbeitet diese gewissenhaft und transparent. Durch die Aufdeckung von Schwachstellen können wir unseren Kunden ein konstant hohes Maß an Sicherheit bieten. Es liegt daher in unserem Interesse, Schwachstellen zu identifizieren und eine zufriedenstellende Lösung zu entwickeln.

Diese Richtlinie zur Offenlegung von Schwachstellen beschreibt das Verfahren, das bei der Meldung von Schwachstellen an uns (die „Organisation“) und bei der Untersuchung unserer Produkte auf Schwachstellen zu befolgen ist.
Wir empfehlen Ihnen, diese Richtlinie zur Offenlegung von Sicherheitslücken vollständig zu lesen, bevor Sie eine Sicherheitslücke melden, und sich stets daran zu halten. Wir schätzen diejenigen, die sich die Zeit und Mühe nehmen, Sicherheitslücken gemäß dieser Richtlinie zu melden. Wir bieten jedoch keine finanziellen Belohnungen für die Offenlegung von Sicherheitslücken.

Die meldende Partei

Die meldende Partei ist für Ihre eigenen Handlungen verantwortlich und muss bei der Untersuchung und Meldung von Schwachstellen die Grundsätze der Verhältnismäßigkeit und Subsidiarität beachten. Mit anderen Worten: Die meldende Partei sollte nicht mehr als nötig tun, um die Schwachstelle nachzuweisen, und sollte die Schwachstelle immer zuerst dem Eigentümer des Systems/der Informationen melden.

Im Gegenzug wird die Organisation keine rechtlichen Schritte gegen Ihre gut gemeinten Untersuchungen und Meldungen von Sicherheitslücken einleiten, wenn Sie die Anweisungen dieser Richtlinie befolgen. Dieser Rechtsschutz gilt nicht, wenn Anzeichen für böswillige Absichten vorliegen.

Die meldende Partei muss
- das Problem so schnell wie möglich melden, um zu verhindern, dass böswillige Dritte die Schwachstelle entdecken und ausnutzen.
- die Meldung vertraulich an die Organisation richten, um zu verhindern, dass andere Zugang zu diesen Informationen erhalten.

Die meldende Partei und die Organisation treffen klare Vereinbarungen über die Offenlegung der Schwachstelle. Sind mehrere Organisationen beteiligt, gilt grundsätzlich, dass die Schwachstellen nur veröffentlicht werden dürfen, wenn alle Organisationen damit einverstanden sind.

Meldung der Sicherheitslücke

Wenn Sie glauben, eine Sicherheitslücke gefunden zu haben, senden Sie uns bitte Ihren Bericht an folgende EMailAdresse: service-support@meiko-global.com

Es können nur EMails in englischer oder deutscher Sprache berücksichtigt werden. Bitte geben Sie in Ihrem Bericht die folgenden Details zur Sicherheitslücke an:

- Asset (Webadresse, IPAdresse, Produkt- oder Dienstleistungsname), bei dem die Sicherheitslücke beobachtet werden kann
- Schwäche (z. B. CWE) (optional)

- Schweregrad (z. B. CVSS v3.1) (optional)
- Bezeichnung der Sicherheitslücke (obligatorisch)
- Beschreibung der Sicherheitslücke (diese sollte eine Zusammenfassung, unterstützende Dateien und mögliche Abhilfemaßnahmen oder Empfehlungen enthalten) (obligatorisch)
- Auswirkungen (Was könnte ein Angreifer tun?) (obligatorisch)
- Schritte zur Reproduktion. Diese sollten harmlos und nicht destruktiv sein und als Proof of Concept dienen.

Optionale Kontaktdaten:
- Name
- EMailAdresse

Was Sie erwarten können

Nachdem Sie Ihren Bericht eingereicht haben, sorgen wir dafür, dass der Bericht gemäß unseren Prozessen, an die am besten geeignete Abteilung weitergeleitet wird. Nach der Einreichung läuft der Prozess wie folgt ab:
- Die Organisation sendet eine Empfangsbestätigung an den Meldenden.
- Der Bericht wird gemäß unserer Risikobewertung (Auswirkungen, Schweregrad, Komplexität der Ausnutzung) bewertet und bearbeitet.
- Die Organisation informiert den Meldenden über den Status.
- Der Meldende sollte davon absehen, häufiger als alle 14 Tage nachzufragen.
- Die Organisation veröffentlicht die Ergebnisse in Absprache mit dem Meldenden, wenn eine begründete Wahrscheinlichkeit besteht, dass die Schwachstelle auch an anderen Stellen vorhanden ist.
- Wir behandeln Ihre Meldung streng vertraulich.
- Wir geben Ihre persönlichen Daten ohne Ihre Zustimmung nicht an Dritte weiter.

Leitfaden

Es ist untersagt:
- Die von Ihnen entdeckte Schwachstelle oder das Problem auszunutzen, beispielsweise durch unnötigen Zugriff, übermäßige oder erhebliche Datenmengen
- Das Problem anderen zu offenbaren, bevor es behoben wurde
- Daten in den Systemen oder Diensten der Organisation zu ändern
- Angriffe auf die physische Sicherheit, Social Engineering, Distributed Denial of Service, Spam oder hochintensive invasive oder destruktive ScanTools verwenden, um Schwachstellen zu finden.
- Jegliche Form von DenialofService versuchen oder melden, z. B. einen Dienst mit einer hohen Anzahl von Anfragen überlasten.
- Die Dienste oder Systeme der Organisation stören.

Kontakt

E-mail: service-support@meiko-global.com