Promicon Elektronik GmbH + Co. KG
Im Michelreis 6
72124 Pliezhausen

Fon +49 (0) 7127-9 37 30
www.promicon.de

TLP:CLEAR

Richtlinie zur koordinierten Offenlegung von Schwachstellen

1 Einleitung

Bei Promicon Elektronik GmbH + Co. KG (weiterhin als Promicon oder Promicon Systems bezeichnet) hat die Sicherheit der eigenen Produkte und Dienstleistungen oberste Priorität. Die Einhaltung von Sicherheitsstandards zum Schutz der Privatsphäre und der Integrität der Daten unserer Kunden ist uns wichtig.

Um die Sicherheit der Systeme unserer Kunden und unserer Produkte zu gewährleisten, bitten wir den Meldenden eine koordinierte Offenlegung vorzunehmen. Zudem die Informationen vertraulich zu behandeln, bis eine Lösung vorliegt, anstatt Schwachstellen sofort auf öffentlichen Plattformen offenzulegen.

Unser Product Security Incident Response Team (weiterhin als Promicon PSIRT bezeichnet) ist bestrebt, alle Meldungen umgehend zu bearbeiten, um die Zuverlässigkeit und Sicherheit der Promicon Produkte weiterhin zu gewährleisten.

Diese Richtlinie zur koordinierten Offenlegung von Schwachstellen beschreibt das Verfahren zur Meldung von Schwachstellen an uns und erläutert, was Meldende im Gegenzug erwarten können.

Bitte lesen Sie diese Richtlinie vollständig durch, bevor Sie eine Schwachstelle melden, und handeln Sie stets in Übereinstimmung mit ihr.

2 Geltungsbereich

Diese Richtlinie gilt für alle von Promicon erstellten aktiven Produkte, unabhängig von ihrem vertraglichen Status oder ihrer Position im Produktlebenszyklus – sei es in der Entwicklungsphase, in der Wartungsphase oder sogar nach Abschluss der Wartung.

Im Zuge einer verantwortlichen Offenlegung bitten wir darum, von folgenden Szenarien abzusehen:

- Physische Angriffe, Social Engineering oder andere nicht technische Schwachstellentests
- Network Denial of Service (DoS oder DDos)-Angriffe oder Tests, die die Verfügbarkeit beeinträchtigen oder beschädigen
- Massenhaft automatisierte Scans
- Schwachstellen-Meldung in Software oder Diensten Dritter, die nicht unter unserer Kontrolle stehen

Bei Unsicherheiten, ob ein Test im Scope liegt, bitten wir um vorherige Rücksprache.

Die Aufgaben des Promicon PSIRT werden vollumfänglich durch die Geschäftsführung unterstützt und liegt im grundsätzlichen Interesse des Unternehmens.

Richtlinie zur koordinierten Offenlegung von Schwachstellen

3 Meldung von Schwachstellen

Schwachstellen können bereits im Rahmen von Patches, neuen Versionen oder Klarstellungen zur Nichtausnutzbarkeit behoben sein. Bitte prüfen Sie vorab, ob Sie diesbezüglich aktuell sind.

Wenn Sie glauben, eine potenzielle Schwachstelle in einem unserer Systeme gefunden zu haben, melden Sie diese bitte per E-Mail an das Promicon PSIRT:

psec-psirt@promicon-systems.de

Damit das Promicon PSIRT die potenzielle Schwachstelle bearbeiten kann, sollten Sie folgende Informationen bereitstellen:

- Vollständiger Produktname und die betroffene Komponente
- Versionsstände von Hardware und Software aller beteiligten Komponenten
- Datum und Uhrzeit des Vorfalls (Zeitzone bitte angeben)
- Detaillierte Beschreibung der Schwachstelle
  - Technische Details (wie z. B. Systemkonfiguration, Protokoll-Daten, Beschreibung des Exploit-/Angriffscodes)
  - Detailierte Schrittkette zur Reproduktion der Schwachstelle
  - Anhänge, die bei der Nachstellung des Problems helfen, wie beispielsweise Bilder, Videos, Skripte und Nutzlast
  - Proof-of-Concept-Code, falls vorhanden
- Einschätzung des Schweregrads der Schwachstelle
- Auswirkungen der Schwachstelle, einschließlich der Art und Weise, wie ein Angreifer die Schwachstelle ausnutzen könnte
- Ihre Kontaktdaten - wir respektieren anonyme Meldungen

Die Informationen sollten auf Deutsch oder Englisch bereitgestellt werden.

Unzureichende Angaben können dazu führen, dass das Promicon PSIRT die Informationen nicht bestätigen kann.

Promicon empfiehlt dem Meldenden, sensible Informationen, die per E-Mail übermittelt werden, zu verschlüsseln. Das Promicon PSIRT unterstützt mit OpenPGP Standard verschlüsselte Nachrichten. Bitte senden Sie uns Ihren PGP-Schlüssel zu, damit Promicon PSIRT Ihnen sicher antworten kann.

Zudem ist das Promicon PSIRT telefonisch unter der Telefonnummer +49 (0) 71 27 - 9 37 30 erreichbar.

Die Geschäftszeiten von Promicon PSIRT beschränken sich in der Regel auf die üblichen Bürozeiten. Diese sind:

09:00 - 16:00 (GMT+0100 und GMT+0200 zur Sommerszeit) von Montag bis Freitag, außer der Ferienzeit in Baden-Württemberg, Deutschland und Betriebsferien.

Richtlinie zur koordinierten Offenlegung von Schwachstellen

Unseren öffentlichen PGP-Schlüssel und den dazugehörigen Fingerabdruck finden Sie auf unseren Webseiten:

https://www.promicon.de/promicon-psirt.html

https://www.promicon-systems.de/promicon-psirt.html

https://www.varimotion.de/promicon-psirt.html

https://www.compactmotion.de/promicon-psirt.html

https://www.vari-move.de/promicon-psirt.html

https://www.promicon.com/promicon-psirt.html

https://www.promicon-systems.com/promicon-psirt.html

https://www.vari-motion.de/promicon-psirt.html

https://www.compact-motion.de/promicon-psirt.html

Wichtige Hinweise

- Wir bearbeiten ausschließlich Informationen zu potenziellen Schwachstellen, die Promicon Produkte betreffen.
- Anonyme Meldungen können nur in begrenztem Umfang oder möglicherweise gar nicht bearbeitet werden, da die Möglichkeit fehlt, technische oder inhaltliche Rückfragen zu stellen.
- Wir werden Ihre Kontaktdaten ausschließlich zur Analyse und Erfassung potenzieller Schwachstellen verwenden. Ihre Kontaktdaten werden nur durch Ihre ausdrückliche Erlaubnis an Dritte weitergegeben.
- Zum Schutz unserer Kunden bitten wir Sie, die Schwachstelle nicht ohne vorherige Absprache mit dem Promicon PSIRT an andere Personen oder Organisationen weiterzugeben.

4 Reaktionszeiten

Wenn Sie sich dazu entscheiden, uns Ihre Kontaktinformationen mitzuteilen, verpflichten wir uns, so offen und schnell wie möglich mit Ihnen zu kommunizieren. Wir bitten Sie jedoch um Verständnis, dass unsere Antwort einige Zeit in Anspruch nehmen kann.

- Wir werden Ihnen innerhalb von fünf Werktagen den Eingang Ihres Berichts bestätigen.
- Wir werden im Rahmen unserer Möglichkeiten versuchen, Ihnen gegenüber das vorhanden sein der Schwachstelle zu bestätigen und Ihnen so transparent wie möglich mitzuteilen, welche Schritte wir im Rahmen der Behebung unternehmen, einschließlich der Probleme oder Herausforderungen, die eine Lösung verzögern.
- Wir werden einen offenen Dialog mit Ihnen führen, um Probleme zu besprechen.

Richtlinie zur koordinierten Offenlegung von Schwachstellen

5 Safe-Harbor

Promicon wird keine rechtlichen Schritte gegen Personen einleiten, die Schwachstellen gemäß dieser Richtlinie aufdecken und melden, sofern diese:

- keinen Schaden gegen Promicon, unseren Kunden oder anderen zufügt
- die Privatsphäre noch die Sicherheit unserer Kunden noch den Betrieb unserer Dienste gefährdet
- nicht gegen Strafgesetze verstoßen
- Details zu Schwachstellen erst veröffentlicht werden, nachdem Promicon den Abschluss der Abhilfemaßnahmen bestätigt hat

6 Anerkennung

Promicon betreibt kein Bug Bounty-Programm. Mit der Bereitstellung von Daten und Informationen bezüglich einer Schwachstelle erkennen Sie an, dass damit keine Zahlungserwartung verbunden ist und dass Sie ausdrücklich auf künftige Zahlungsanforderungen gegen Promicon in Bezug auf Ihre Bereitstellung verzichten.

Promicon bietet zwar kein Bug Bounty-Programm oder eine sonstige Vergütung an, erkennt jedoch die Beiträge von Sicherheitsforschern an und weiß sie zu schätzen.

Änderungen an dieser Richtlinie

Promicon behält sich das Recht vor, diese Richtlinie jederzeit ohne vorherige Ankündigung zu ändern. Wir empfehlen Ihnen, diese Seite regelmäßig auf Aktualisierungen zu überprüfen.