SEG
an Arteche Company

Richtlinie zur Meldung von Sicherheitslücken

September 2026

01

Richtlinie zur Meldung von Sicherheitslücken

Bei SEG hat die Sicherheit unserer Produkte höchste Priorität. Wir sind uns bewusst, dass erkannte und ausgenutzte Sicherheitslücken die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme und/oder Anwendungen gefährden können, in denen Produkte von Arteche eingesetzt werden.
Diese Richtlinie zur Meldung von Sicherheitslücken (Vulnerability Disclosure Policy) beschreibt, welche Systeme und Arten von Tests autorisiert sind. Wir bitten Sie, Informationssicherheitsprobleme verantwortungsvoll und im Einklang mit dieser Richtlinie zu melden.

02

Autorisierung

Forschende und Sicherheitsexperten sollen sich sicher fühlen, uns entdeckte Sicherheitslücken gemäß dieser Richtlinie zu melden. Sofern das Verfahren bei der Meldung von Sicherheitsproblemen an die Arteche Group ordnungsgemäß eingehalten wird, werden wir keine rechtlichen Schritte einleiten und Ihren Zugriff auf unsere Produkte und/oder Anwendungen nicht sperren.
SEG behält sich bei Verstößen gegen diese Richtlinie sämtliche gesetzlichen Rechte vor.

03

Geltungsbereich

Diese Richtlinie gilt für Produkte, die digitale Komponenten der Arteche Group verwenden:

- Steuerungsgeräte
- Schutzgeräte
- Messgeräte
- Sensorgeräte

Nicht aufgeführte Services sind vom Geltungsbereich ausgeschlossen und dürfen ohne unsere ausdrückliche Genehmigung nicht getestet werden. Sicherheitslücken, die in Geräten von Drittanbietern festgestellt werden, sind ebenfalls vom Geltungsbereich ausgeschlossen und sollten direkt dem jeweiligen Anbieter oder Hersteller gemäß dessen eigener Richtlinie zur Meldung von Sicherheitslücken gemeldet werden.

04

Richtlinien

4.1. Pflichten bei der Durchführung Ihrer Untersuchungen oder Tests

- Greifen Sie nicht unbefugt auf Produktivsysteme zu. Sollte der Zugriff versehentlich erfolgen oder ein System öffentlich zugänglich sein, informieren Sie die für die Infrastruktur, in der das betreffende Gerät installiert ist, verantwortliche Person, csirt@segelectronics.de oder das zuständige CSIRT.
- Nutzen Sie die entdeckte Sicherheitslücke oder das festgestellte Problem nicht aus. Laden Sie beispielsweise nicht mehr Daten herunter, als zum Nachweis der Sicherheitslücke erforderlich sind, und löschen oder verändern Sie keine Daten.
- Verwenden Sie ausschließlich harmlose Anwendungen, Tools oder Payloads, und nur dann, wenn dies zur Bestätigung des Vorhandenseins einer Sicherheitslücke erforderlich ist.
- Veröffentlichen Sie keine bei der Untersuchung heruntergeladenen Daten und geben Sie diese auch nicht an Dritte weiter.
- Wenn Sie auf sensible Informationen stoßen, beispielsweise personenbezogene Daten, Finanz- oder vertrauliche Informationen oder Geschäftsgeheimnisse, brechen Sie die Tests sofort ab, informieren Sie uns und geben Sie die erlangten Daten an niemanden weiter.

4.2. Unzulässige Handlungen

- Das Einbringen von Schadsoftware (Viren, Würmer, Trojaner usw.) in ein Produkt und/oder die Infizierung von Personen, die am Lebenszyklus eines Produkts beteiligt sind.
- Das Gefährden eines Systems durch den Einsatz von Angriffsprogrammen, um die vollständige oder teilweise Kontrolle darüber zu erlangen.
- Das Kopieren, Verändern oder Löschen von Produktdaten.
- Das Vornehmen von Änderungen an Produkten.
- Das wiederholte Zugreifen auf ein Produkt oder das Weitergeben von Zugriffsrechten an die Öffentlichkeit oder an Dritte.
- Die Nutzung eines erlangten Zugriffs, um den Zugriff auf andere Systeme zu versuchen.
- Das Ändern der Zugriffsrechte anderer Benutzer.
- Die Verwendung von Brute-Force- oder Wörterbuchangriffen, um auf ein Produkt zuzugreifen.
- Der Einsatz von Denial-of-Service-Techniken (DoS).
- Der Einsatz von Social-Engineering-Techniken (Phishing, Vishing, Spam usw.).
- Der Einsatz physischer Angriffe auf die Sicherheit.

4.3. Rechtliche Hinweise

Als Teil der Arteche Group wendet die SEG Electronics GmbH den rechtlichen Rahmen der Arteche Group für die Meldung von Sicherheitslücken an. Die folgenden rechtlichen Anforderungen werden unverändert übernommen.

Diese Richtlinie steht im Einklang mit den anerkannten bewährten Verfahren für die Meldung von Sicherheitslücken. Sie berechtigt Sie nicht zu Handlungen, die gegen geltendes Recht verstoßen oder dazu führen könnten, dass Arteche gegen gesetzliche Verpflichtungen verstößt.

Anwendbare Gesetze und regulatorische Anforderungen:

- die Datenschutz-Grundverordnung (DSGVO) (EU) 2016/679;
- die Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act, CRA) (EU) 2024/2847;

04

Richtlinien

- die jeweils anwendbaren nationalen Datenschutzgesetze;
- die gesetzlichen Bestimmungen zum Schutz geistiger Eigentumsrechte und des Urheberrechts;
- die gesetzlichen Bestimmungen zum Schutz von Geschäftsgeheimnissen und vertraulichen Geschäftsinformationen;
- die jeweils anwendbaren Gesetze und Vorschriften zur Cybersicherheit, zur missbräuchlichen Nutzung von Computersystemen und zum unbefugten Zugriff;
- alle sonstigen anwendbaren regulatorischen Anforderungen, die für SEG-Produkte und deren Einsatzumgebung relevant sind.