acontis technologies GmbH

SOFTWARE

Coordinated Vulnerability Disclosure (CVD) Policy

According to EU-CRA

Revision 1

Contents

1. Deutsche Fassung

Die Sicherheit unserer Produkte hat bei Acontis höchste Priorität. Trotz sorgfältiger Entwicklung können Schwachstellen niemals vollständig ausgeschlossen werden. Wenn Sie in einem unserer Produkte eine Schwachstelle entdecken, möchten wir davon erfahren, um sie zügig beheben zu können. Diese Richtlinie beschreibt, wie Sie eine Schwachstelle melden, was Sie von uns erwarten können und welche Spielregeln dabei gelten.

Wir folgen dem Prinzip der koordinierten Offenlegung (Coordinated Vulnerability Disclosure) und orientieren uns an anerkannten Standards (u. a. ISO/IEC 29147 und 30111) sowie an den Vorgaben des EU Cyber Resilience Act.

1.1. Zusammenfassung

Direkte Ansprechpartner: Melden Sie Schwachstellen direkt an security@acontis.com (menschenüberwacht; nicht vollständig automatisiert).

- Sie erhalten eine Bestätigung nach Empfang und einer ersten Kontrolle unsererseits, spätestens innerhalb von 5 Tagen
- Koordinierte Behebung der Schwachstelle innerhalb von 90 Tagen
- Offenlegung nach der Behebung der Schwachstelle

1.2. Geltungsbereich

Diese Richtlinie **gilt für alle derzeit unterstützten Produkte und Softwarelösungen von acontis**, einschließlich, aber nicht beschränkt auf, EC-Master, EC-Engineer, EC-Simulator, EC-Inspector, LxWin und RTOSVisor. Sie gilt außerdem auch für **Drittanbieterkomponenten,** welche in Acontis-Softwareprodukte integriert sind als auch **öffentliche Webdienste, welche von Acontis betrieben werden.**

Diese Richtlinie **deckt in der Regel keine Produkte ab,** deren Supportzeitraum abgelaufen ist (End-of-Life), ebenso Schwachstellen in Drittanbieterkomponenten welche nicht integriert oder von acontis geliefert werden (bitte melden Sie diese bitte dem jeweiligen Anbieter), Angriffe auf physische Sicherheit, Social Engineering, Phishing und (Distributed-)Denial-of-Service-Tests und Befunde ohne realistische sicherheitsrelevante Auswirkung (z. B. fehlende „Best-Practice"-Header ohne nachweisbares Risiko)

Im Zweifelsfall melden Sie das Ergebnis bitte trotzdem – wir werden es prüfen.

1.3. Wie Sie eine Schwachstelle melden

Bitte senden Sie Ihre Meldung an:

- **Email:** security@acontis.com
- **Web:** www.acontis.com/security/cvereport
- **security.txt:** https://www.acontis.com/.well-known/security.txt (gemäß RFC 9116)

1.4. Was Ihre Meldung enthalten sollte

Um uns zu helfen, das Problem schnell nachzuvollziehen und zu beheben, geben Sie bitte nach Möglichkeit folgende Informationen an:

- Das betroffene Produkt: Produktname oder Acontis-Artikelcode und Versionsnummer
- Eine detaillierte technische Beschreibung der potenziellen Schwachstelle, einschließlich bekannter verwandter Exploits.
- Schritt-für-Schritt-Anweisungen zur Reproduktion des Problems (Proof-of-Concept, Screenshots oder Logs sind herzlich willkommen)
- Alle damit verbundenen öffentlichen Offenlegungen (CVE, Empfehlungen, wissenschaftliche Arbeiten).

- Falls bekannt: eine Einordnung nach CWE und/oder eine CVSS-Einschätzung
- Ihre Kontaktdaten für Rückfragen und – falls gewünscht – ob Sie genannt werden möchten

Berichte werden vertraulich behandelt und über sichere Kanäle übertragen. Bitte vermeiden Sie es, sensible personenbezogene Daten anzugeben.
Alle persönlichen Daten von Meldern – einschließlich Namen, E-Mails oder anderer Kontaktdaten – werden gemäß der EU-Datenschutzverordnung (DSGVO) verarbeitet. Daten werden ausschließlich zur koordinierten Offenlegung von Schwachstellen verwendet, streng vertraulich behandelt und gelöscht, wenn sie für regulatorische oder kommunikative Zwecke nicht mehr erforderlich sind.

Meldungen auf Deutsch oder Englisch sind gleichermaßen willkommen.

1.5. Unser Prozess und was Sie erwarten können

Nach Erhalt eines Schwachstellenberichts verpflichtet sich acontis zu folgendem Prozess:

- **Bestätigung des Empfangs:** typischerweise innerhalb von 24 Stunden (automatisiert).
- **Erste inhaltliche Antwort / Triage:** innerhalb von fünf Werktagen.
- **Bewertung:** Jeder Bericht wird von unseren Sicherheitsexperten überprüft, priorisiert und bewertet, um die betroffenen Produkte zu bestimmen und die Schwere mittels CVSS zu bewerten.
- **Zusammenarbeit:** Wir können Sie für weitere technische Informationen oder Klarstellungen kontaktieren.
- **Status-Updates:** Wir halten Sie über wichtige Meilensteine informiert (Bestätigung, geplante Sanierung, Veröffentlichung).
- **Vertraulichkeit:** Details der Schwachstelle bleiben vertraulich, bis eine Lösung vorliegt.
- **Behebung:** Unser Ziel ist es, gültige Schwachstellen innerhalb von 90 Tagen zu beheben. Komplexe Fälle benötigen möglicherweise mehr Zeit, in diesem Fall werden regelmäßig Statusupdates bereitgestellt, typischerweise alle 30 Tage.

1.6. Offenlegung und Kommunikation

Sobald eine Lösung verfügbar ist und Updates an Kunden veröffentlicht werden, veröffentlicht Acontis eine Sicherheitswarnung auf unserer Website. Die Warnung enthält eine CVE-Kennung (sofern zutreffend), eine Zusammenfassung des Problems, betroffener Produkte und Versionen, Schwere (CVSS v4.0), Sanierungsanweisungen und Verfügbarkeit von Patches.

Wenn eine gemeldete Schwachstelle Drittanbieter-Software betrifft, koordinieren wir die Offenlegung mit den zuständigen Anbietern, um einen verantwortungsvollen Umgang mit allen betroffenen Produkten sicherzustellen.

Wenn Acontis von einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall erfährt, werden betroffene Nutzer und relevante öffentliche Stellen ohne unnötige Verzögerung über das Problem sowie über alle verfügbaren Risikominderungs- oder Korrekturmaßnahmen informiert, selbst wenn eine vollständige Lösung noch nicht verfügbar ist.

1.7. Grundsätze der verantwortungsvollen Offenlegung

Um eine sichere und konstruktive Zusammenarbeit zwischen Sicherheitsforschern und acontis zu gewährleisten, bitten wir alle Parteien, die folgenden Grundsätze zur Offenlegung einzuhalten:

- Nutzen Sie die Schwachstelle nicht für unbefugten Datenzugriff.
- Vermeiden Sie jegliche Aktivitäten, die die Verfügbarkeit von Produkten oder Dienstleistungen beeinträchtigen könnten.
- Respektieren Sie jederzeit die Privatsphäre der Nutzer sowie die Datenschutzbestimmungen.
- Veröffentlichen Sie die Schwachstelle nicht öffentlich vor einer koordinierten Veröffentlichung mit Acontis.

1.8. Leitsätze für die Untersuchung

Wir bitten Sie, bei Ihrer Untersuchung Folgendes zu beachten:

- Greifen Sie nur auf so viele Daten zu, wie zum Nachweis der Schwachstelle nötig ist.
- Verändern oder löschen Sie keine Daten und beeinträchtigen Sie nicht die Verfügbarkeit unserer Systeme oder die unserer Kunden oder Partner.
- Nutzen Sie keine Methoden, die über das zum Nachweis Erforderliche hinausgehen (z. B. keine Spam-, DoS- oder Social-Engineering-Angriffe).
- Geben Sie die Schwachstelle erst nach Abstimmung mit uns öffentlich bekannt.
- Beachten Sie geltendes Recht.

1.9. Rechtlicher Rahmen (Safe Harbor)

acontis wird keine rechtlichen Schritte gegen Personen einleiten, die Schwachstellen in gutem Glauben und in Übereinstimmung mit dieser Richtlinie identifizieren und melden. Forschungsaktivitäten dürfen weder vorsätzlich Schaden verursachen noch auf Daten zugreifen, die über das hinausgehen, was zum Nachweis des Problems erforderlich ist.

Diese Richtlinie berechtigt nicht zur Durchführung von Penetrationstests an der Infrastruktur von acontis ohne vorherige schriftliche Zustimmung seitens acontis. Dieser Abschnitt findet zudem keine Anwendung bei erkennbar böswichtiger Absicht oder Handlungen zum persönlichen Vorteil.

1.10. Anerkennung

Acontis bietet derzeit kein Bug-Bounty-Programm an und zahlt keine Prämien. Wir nennen Sie jedoch gerne als Entdecker der Schwachstelle in unserem Sicherheits-Advisory, sofern Sie dies wünschen.

1.11. Sicherheitsupdates und Support

Sicherheitsupdates für unterstützte Acontis-Produkte werden für mindestens fünf Jahre ab der Erstveröffentlichung des Produkts oder – falls kürzer – die vorgesehene Produktlebensdauer kostenlos bereitgestellt. Jeder Hinweis enthält detaillierte Anweisungen und, falls verfügbar, Download-Links für relevante Patches oder Updates.

1.12. Information zu rechtlichen Verpflichtungen

Diese Richtlinie beschreibt unseren freiwilligen Prozess zur koordinierten Offenlegung. Sie beschreibt nicht die gesetzlichen Melde- und Offenlegungspflichten – wie etwa die Meldepflichten von Herstellern gemäß dem EU Cyber Resilience Act gegenüber dem zuständigen CSIRT und der ENISA.

1.13. Kontaktdaten

Acontis pflegt diese Kontakte für Schwachstellenmeldungen und damit Nutzer Informationen über Schwachstellen in Acontis-Produkten mit digitalen Elementen erhalten:

- **Email:** security@acontis.com
- **Web:** www.acontis.com/security/cvereport
- **security.txt:** https://www.acontis.com/.well-known/security.txt (per RFC 9116)

acontis hält diese Kontaktmöglichkeit leicht zugänglich, weist klar auf deren Verfügbarkeit hin (gegebenenfalls auch in den Produktinformationen für Nutzer) und hält diese Informationen aktuell. Sofern für Sicherheitsanfragen automatisierte Tools (z. B. Chat) angeboten werden, wird zusätzlich eine Telefonnummer

und/oder ein weiteres digitales Kontaktmittel (z. B. E-Mail oder Kontaktformular) bereitgestellt; die genannten Kontaktstellen stützen sich somit nicht ausschließlich auf automatisierte Tools.

1.14. Weitere Fragen

Bei Fragen zu dieser Richtlinie oder zum koordinierten Offenlegungsprozess wenden Sie sich bitte an unser Sicherheitsteam über die oben genannte E-Mail-Adresse.

1.15. Sprachvarianten und Änderungen dieser Richtlinie

Bei Unterschieden zwischen der englischen und der deutschen Version gilt die deutsche Version.

Wir können diese Richtlinie jederzeit aktualisieren. Es gilt die auf unserer Website veröffentlichte Version. Den Versionsstatus entnehmen Sie bitte der Dokumentenkopfzeile.

2. English version

The security of our products is a high priority at acontis. Despite careful development, vulnerabilities can never be fully ruled out. If you discover a vulnerability in one of our products, we want to hear about it so we can address it quickly. This policy explains how to report a vulnerability, what you can expect from us, and the rules that apply.

We follow the principle of Coordinated Vulnerability Disclosure and align with recognized standards (including ISO/IEC 29147 and 30111) as well as the requirements of the EU Cyber Resilience Act.

2.1. Summary

Single point of contact: Report vulnerabilities to security@acontis.com (human-monitored; not exclusively automated).

- Acknowledgment provided after reception and first check, latest within 5 days
- Coordinated remediation within 90 days
- Public advisory after remediation is available

2.2. Scope

This policy **applies to all acontis products and software solutions which are currently supported**, including but not limited to EC-Master, EC-Engineer, EC-Simulator, EC-Inspector, LxWin, and RTOSVisor. It also **covers third-party components integrated** within acontis software products **and public web services operated by acontis.**

This policy **typically does not cover** products whose support period has ended (end-of-life), vulnerabilities in third-party components that are not integrated or shipped by acontis (please report these to the respective vendor), attacks on physical security, social engineering, phishing, and (distributed) denial-of-service testing and findings without a realistic security impact (e.g. missing "best-practice" headers with no demonstrable risk)

If in doubt, please report the finding anyway — we will assess it.

2.3. How to report a vulnerability

Please send your report to:

- **Email:** security@acontis.com
- **Web:** www.acontis.com/security/cvereport
- **security.txt:** https://www.acontis.com/.well-known/security.txt (per RFC 9116)

2.4. What your report should include

To help us reproduce and fix the issue quickly, please include the following information where possible:

- The affected product: Product name or acontis item code and version number
- A detailed technical description of the potential vulnerability, including known related exploits.
- Step-by-step instructions to reproduce the issue (proof-of-concept, screenshots or logs are highly welcome)
- Any related public disclosures (CVE, advisories, academic papers).
- If known: a CWE classification and/or a CVSS estimate
- Your contact details for follow-up questions and — if desired — if you wish to be credited

Reports are handled confidentially and transmitted over secure channels. Please avoid including sensitive personal data.
Any personal data of reporters—including names, emails, or other contact details—will be processed in

compliance with the EU General Data Protection Regulation (GDPR). Data is used solely to facilitate coordinated vulnerability disclosure, kept strictly confidential, and deleted when no longer required for regulatory or communication purposes.

Reports in German or English are equally welcome.

2.5. Our process and what to expect

Upon receiving a vulnerability report, acontis commits to the following process:

- **Acknowledgement of receipt:** typically, within 24 hours (automated).
- **First substantive response / triage:** within five business days.
- **Assessment:** Each report will be reviewed, prioritized, and evaluated by our security experts, to determine the affected products and rate severity using CVSS.
- **Collaboration:** We may contact you for further technical information or clarification.
- **Status updates:** We keep you informed at key milestones (confirmation, planned remediation, publication).
- **Confidentiality:** Details of the vulnerability will remain confidential until a fix is available.
- **Remediation:** Our goal is to resolve valid vulnerabilities within 90 days. Complex cases may require more time, in which case status updates will be provided regularly, typically every 30 days.

2.6. Disclosure and Communication

Once a fix is available and updates are released to customers, acontis will publish a security advisory on our website. The advisory will include a CVE identifier (if applicable), a summary of the issue, affected products and versions, severity (CVSS v4.0), remediation instructions, and patch availability.

If a reported vulnerability affects third-party software, we will coordinate disclosure with the relevant vendors to ensure responsible handling across all affected products.

Where acontis becomes aware of an actively exploited vulnerability or a severe security incident, affected users and relevant public bodies will be informed without undue delay about the issue and any available risk mitigation or corrective measures, even if a full fix is not yet available.

2.7. Responsible Disclosure Principles

To ensure a safe and constructive collaboration between security researchers and acontis, we ask all parties to adhere to the following responsible disclosure principles:

- Do not exploit or use the vulnerability for unauthorized data access.
- Avoid any activity that could degrade product or service availability.
- Respect user privacy and data protection regulations at all times.
- Do not publicly disclose the vulnerability before coordinated publication with acontis.

2.8. Rules of engagement

When investigating, we ask you to:

- Access only as much data as is necessary to demonstrate the vulnerability.
- Not alter or delete data, and not impair the availability of our systems or those of our customers or partners.
- Not use methods beyond what is necessary to demonstrate the issue (no spam, DoS or social-engineering attacks).
- Not disclose the vulnerability publicly until coordinated with us.

- Comply with applicable law.

2.9. Legal framework (safe harbor)

acontis will not pursue legal action against individuals who identify and report vulnerabilities in good faith and in compliance with this policy. Research activities must not intentionally cause harm or access data beyond what is required to demonstrate the issue.

This policy does not authorize penetration testing of acontis infrastructure without prior written consent. This section does not apply where there is recognizable malicious intent or action for personal gain.

2.10. Recognition

acontis does not currently operate a bug bounty program and does not pay rewards. However, we are happy to credit you as the discoverer of the vulnerability in our security advisory, if you wish.

2.11. Security Updates and Support

Security updates for supported acontis products are provided free of charge for at least five years from the product's initial release or, if shorter, the intended product lifetime. Each advisory includes detailed instructions and, if available, download links for relevant patches or updates.

2.12. Relationship to legal obligations

This policy describes our voluntary coordinated disclosure process. It does not affect statutory reporting and disclosure obligations — such as manufacturers' reporting duties under the EU Cyber Resilience Act towards the relevant CSIRT and ENISA.

2.13. Contact

acontis maintains point of contacts as listed below for vulnerability reporting and for users to receive information about vulnerabilities in acontis products with digital elements:

- **Email:** security@acontis.com
- **Web:** www.acontis.com/security/cvereport
- **security.txt:** https://www.acontis.com/.well-known/security.txt (per RFC 9116)

acontis keeps this contact easily accessible, clearly indicates its availability (including in product user information where applicable), and keeps this information up to date. Where automated tools (e.g. chat) are offered for security enquiries, a phone number and/or another digital means of contact (e.g. email or contact form) is also provided; the mentioned point of contacts do not rely exclusively on automated tools.

2.14. Questions

For questions regarding this policy or the coordinated disclosure process, please contact our security team via the above email address.

2.15. Prevailing version and changes to this policy

In case of differences between the English and the German version, the German version shall prevail.

We may update this policy at any time. The version published on our website applies. See the document header for the version status.