Vulnerability Disclosure Policy at manroland Goss Group

Purpose

manroland Goss values the security of our products. We encourage security researchers, customers, and any other third parties to report vulnerabilities responsibly so we can investigate and remediate them in a coordinated manner.

This policy explains how to report vulnerabilities to us, what to expect after reporting, and what testing activities are permitted.

Scope

This policy applies to all manroland Goss products.

Out of scope:

- Third-party systems not produced, included or operated by manroland Goss.
- Products that are no longer supported.
- Social engineering, physical attacks, and spam against employees or customers.
- Purely theoretical vulnerabilities that are not exploitable in the context of our concrete product, for example, as generated by an automated vulnerability scanner.
- Findings based solely on the presence of outdated third-party components (e.g. libraries, frameworks, web servers, operating systems), unless the issue can be shown to affect our concrete product in a meaningful and exploitable way.
- Generic hardening observations, for example, TLS configuration preferences, unless they result in an exploitable security weakness in our concrete product.

How to report

Please report vulnerabilities.

We support PGP/GPG encryption:

- PGP public key: https://www.manrolandgoss.com/files/mgws/security/public-key-manrolandgoss.asc

Please include:

- A clear description of the issue.
- The affected product and version number.
- Steps to reproduce.
- Proof-of-concept code, logs, screenshots, or videos, if helpful.
- Your contact details, if you want a response.

If you believe the issue is actively exploited, please state that in your report.

What is allowed

We consider the following research activities to be acceptable when conducted in good faith, with reasonable care, and in compliance with this policy:

- Testing only against in-scope systems.
- Using non-destructive methods.
- Accessing only the minimum data needed to demonstrate the issue.
- Stopping once the vulnerability is confirmed.
- Reporting the issue promptly and privately.

What is not allowed

The following activities are prohibited unless we have given prior written authorisation:

- Exfiltrating, modifying, or deleting user, customer or company data.
- Persistently accessing systems or accounts.
- Disrupting service availability or degrading performance.
- Pivoting to other systems or accounts.
- Using the vulnerability to extort, threaten, or embarrass the manufacturer or their customers.
- Public disclosure before we have had a reasonable opportunity to address the issue, except where required by law or where immediate disclosure is necessary to prevent harm.

Our commitment

When you report a vulnerability in good faith and in accordance with this policy, we will:

- Triage the report and assess the impact.
- Keep you informed of progress, where appropriate and if desired.
- Coordinate remediation and, where feasible, publication.

- Recognise your contribution, if you request credit and we agree it is appropriate.
- We do not operate a bug bounty programme and do not offer monetary compensation for vulnerability reports.
- We will not initiate legal action against individuals who act in good faith and follow this policy.

Timeline and coordination

Our goal is to handle reports efficiently and transparently. Typical milestones are:

- Acknowledgement of receipt: within 1 business day.
- Initial assessment: within 3 business days.
- Status update: as needed, especially if remediation takes longer.
- Coordinated disclosure: agreed with the reporter, taking into account risk to users and operational constraints.

Vulnerability Disclosure Policy in der manroland Goss Gruppe

Zweck

manroland Goss legt großen Wert auf die Sicherheit unserer Produkte. Wir ermutigen Sicherheitsforscher, Kunden und sonstige Dritte, Schwachstellen verantwortungsvoll zu melden, damit wir sie untersuchen und koordiniert beheben können.

Diese Richtlinie erläutert, wie Sie Schwachstellen an uns melden, was Sie nach einer Meldung erwarten können und welche Testaktivitäten zulässig sind.

Anwendungsbereich

Diese Richtlinie gilt für alle Produkte von manroland Goss.

Nicht im Anwendungsbereich:

- Systeme Dritter, die nicht von manroland Goss hergestellt, eingebunden oder betrieben werden.
- Produkte, die nicht mehr unterstützt werden.
- Social Engineering, physische Angriffe und Spam gegen Mitarbeitende oder Kunden.
- Rein theoretische Schwachstellen, die im Kontext unseres konkreten Produkts nicht ausnutzbar sind, beispielsweise Ergebnisse automatisierter Schwachstellen-Scanner.
- Feststellungen, die ausschließlich auf dem Vorhandensein veralteter Komponenten Dritter beruhen (z. B. Bibliotheken, Frameworks, Webserver, Betriebssysteme), sofern nicht nachgewiesen werden kann, dass sich das Problem in relevanter und ausnutzbarer Weise auf unser konkretes Produkt auswirkt.
- Allgemeine Härtungshinweise, beispielsweise Präferenzen zur TLS-Konfiguration, sofern sie nicht zu einer ausnutzbaren Sicherheitsschwäche in unserem konkreten Produkt führen.

Meldung von Schwachstellen

Bitte melden Sie Schwachstellen.

Wir unterstützen die Verschlüsselung per PGP/GPG:

- Öffentlicher PGP-Schlüssel: manrolandgoss.com/files/mgws/security/public-key-manrolandgoss.asc

Bitte geben Sie an:

- Eine klare Beschreibung des Problems.
- Das betroffene Produkt und die Versionsnummer.
- Schritte zur Reproduktion.
- Proof-of-Concept-Code, Protokolle, Screenshots oder Videos, sofern hilfreich.
- Ihre Kontaktdaten, wenn Sie eine Rückmeldung wünschen.

Wenn Sie davon ausgehen, dass die Schwachstelle aktiv ausgenutzt wird, weisen Sie in Ihrer Meldung bitte darauf hin.

Was erlaubt ist

Wir betrachten die folgenden Forschungsaktivitäten als zulässig, sofern sie in gutem Glauben, mit angemessener Sorgfalt und in Übereinstimmung mit dieser Richtlinie durchgeführt werden:

- Tests ausschließlich gegen Systeme im Anwendungsbereich.
- Verwendung nicht destruktiver Methoden.
- Zugriff ausschließlich auf die Daten, die zum Nachweis des Problems zwingend erforderlich sind.
- Beendigung der Tests, sobald die Schwachstelle bestätigt ist.
- Unverzügliche und vertrauliche Meldung des Problems.

Was nicht erlaubt ist

Die folgenden Aktivitäten sind untersagt, sofern wir keine vorherige schriftliche Genehmigung erteilt haben:

- Exfiltrieren, Verändern oder Löschen von Nutzer-, Kunden- oder Unternehmensdaten.
- Dauerhafter Zugriff auf Systeme oder Konten.
- Beeinträchtigung der Verfügbarkeit von Diensten oder Verschlechterung der Leistung.
- Ausweitung des Zugriffs auf andere Systeme oder Konten.
- Nutzung der Schwachstelle, um den Hersteller oder dessen Kunden zu erpressen, zu bedrohen oder öffentlich zu beschädigen.
- Veröffentlichung, bevor wir eine angemessene Gelegenheit zur Behebung des Problems hatten, außer soweit gesetzlich vorgeschrieben oder soweit eine unverzügliche Veröffentlichung zur Schadensabwehr erforderlich ist.

Unsere Zusagen

Wenn Sie eine Schwachstelle in gutem Glauben und im Einklang mit dieser Richtlinie melden, werden wir:

- die Meldung sichten und die Auswirkungen bewerten.
- Sie über den Fortschritt informieren, soweit angemessen und gewünscht.
- die Behebung und, soweit möglich, die Veröffentlichung koordinieren.
- Ihren Beitrag anerkennen, sofern Sie eine Nennung wünschen und wir sie für angemessen halten.
- Wir betreiben kein Bug-Bounty-Programm und bieten keine finanzielle Vergütung für Schwachstellenmeldungen.
- Wir werden keine rechtlichen Schritte gegen Personen einleiten, die in gutem Glauben handeln und diese Richtlinie befolgen.

Zeitplan und Koordination

Unser Ziel ist eine effiziente und transparente Bearbeitung von Meldungen.
Typische Meilensteine sind:

- Bestätigung des Eingangs: innerhalb von 1 Arbeitstag.
- Erstbewertung: innerhalb von 3 Arbeitstagen.
- Statusaktualisierung: nach Bedarf, insbesondere wenn die Behebung länger dauert.
- Koordinierte Veröffentlichung: abgestimmt mit dem Meldenden, unter Berücksichtigung des Risikos für Nutzer und operativer Randbedingungen.