Cybersecurity@GROB

GROB VULNERABILITY DISCLOSURE GUIDELINE (CVD-PROZESS)

Die GROB-WERKE GmbH & Co. KG setzt sich für höchste Sicherheitsstandards ein. Unsere Produkte und Systeme werden kontinuierlich überwacht und auf Schwachstellen geprüft, um Cyberrisiken zu minimieren. Diese Richtlinie beschreibt unseren Prozess zur koordinierten Schwachstellenoffenlegung (Coordinated Vulnerability Disclosure, CVD) basierend auf den Anforderungen des EU Cyber Resilience Act (CRA). Geltungsbereich & Referenzen: Diese Richtlinie gilt für alle Produkte mit digitalen Elementen (PDE), die von GROB entwickelt, hergestellt oder unter eigenem Namen vermarktet werden – einschließlich Software, eingebetteter Systeme, vernetzter OT-Komponenten sowie integrierter Drittthersteller-Komponenten. Sie orientiert sich an: ISO/IEC 29147 (Vulnerability Disclosure), ISO/IEC 30111 (Vulnerability Handling Processes), dem CRA (Regulation (EU) 2024/2847) sowie BSI TR-03183 (Vulnerability Reports and Notifications).

1. Meldung von Schwachstellen

Sicherheitsforscher, Kunden, Partner und andere Organisationen können potenzielle Schwachstellen über folgende Kanäle melden:

- E-Mail: psirt@grob.de (PGP-verschlüsselte Kommunikation empfohlen; PGP-Schlüssel: 7F26 17DE A093 7F83 3F8E)
- Web-Formular (bevorzugt): (https://www.grobgroup.com/unternehmen/cybersecurity/psirt)
- Security.txt gem. RFC 9116: (https://www.grobgroup.com/.well-known/security.txt)

Eine anonyme Meldung ist möglich. Bitte beachten Sie, dass dadurch keine Rückfragen möglich sind. Für eine Verifikation und Bewertung benötigen wir daher möglichst präzise und vollständige technische Angaben.

Die Meldung sollte folgende Informationen enthalten (Pflichtfelder mit *):

- Titel der Meldung*
- Name, E-Mail-Adresse (optional bei anonymen Meldungen)
- Organisation (falls zutreffend)
- Betroffenes Produkt inkl. Versionsstand*
- GM-Nummer vom Typenschild*
- Ursprünglicher Hersteller bei Drittherstellerkomponenten
- Artikelnummer (nur Hardwarekomponenten von Drittherstellern)
- Technische Beschreibung der Schwachstelle* (betroffene Komponenten, Dienste, Schnittstellen, Parameter, Versionen etc.)
- Schritte zur Reproduktion* (PoC, Exploit-Code, Befehle, Skripte, Konfigurationen)
- CVSS-Vektor (v4.0)*
- Bekannte Gegenmaßnahmen/Workarounds (falls vorhanden)
- Auswirkungen (falls bekannt)

Hinweis: Falls es sich nicht um eine Schwachstelle, sondern um einen technischen Fehler handelt, wenden Sie sich bitte an unseren technischen Support.

GROB-WERKE GmbH & Co. KG • Industriestraße 4 • 87719 Mindelheim
+49 (8261) 996-0 • psirt@grob.de

www.grobgroup.com

Cybersecurity@GROB

GROB VULNERABILITY DISCLOSURE GUIDELINE (CVD-PROZESS)

2. Analyse & Bewertung

Nach Eingang der Meldung durchläuft sie folgende Schritte:

- Eingangsbestätigung durch das PSIRT (i. d. R. innerhalb von 2 Werktagen)
- Prüfung auf Vollständigkeit und Relevanz; Validierung der Meldung
- Technische Analyse gemeinsam mit Entwicklungs- und Qualitätsteams
- Bewertung der Kritikalität (CVSS v4.0) und interne Risikoanalyse
- Regelmäßige Statusupdates an die meldende Person.

3. Behebung der Schwachstelle

Basierend auf der Bewertung werden Maßnahmen zur Behebung eingeleitet (Entwicklung und Test von Sicherheitsupdates, Workarounds, Konfigurationshinweise).

Aktiv ausgenutzte Schwachstellen (Known Exploited)
Bei bestätigter aktiver Ausnutzung wird der Fall bei GROB priorisiert behandelt. Eine koordinierte technische Bearbeitung erfolgt umgehend, sodass innerhalb von 14 Tagen entweder eine endgültige Lösung oder eine risikomindernde Zwischenmaßnahme bereitsteht.

Alle übrigen Schwachstellen (nicht aktiv ausgenutzt)
Für alle anderen gemeldeten Schwachstellen gilt ein branchenübliches, risikoorientiertes Ziel: Bereitstellung eines Patches oder einer wirksamen Risikominderung innerhalb von 90 Kalendertagen. Ist innerhalb von 90 Tagen keine Behebung möglich, veröffentlicht GROB risikomindernde Zwischenlösungen und kommuniziert den weiteren Zeitplan transparent.

4. Meldepflichten bei aktiv ausgenutzten Schwachstellen

Bei aktiv ausgenutzten Schwachstellen erfolgt bei GROB eine priorisierte Behandlung.
Zusätzlich gelten die CRA Meldepflichten:

- Frühwarnung innerhalb von 24 Stunden an die zuständigen Behörden (ENISA & nationales CSIRT).
- Vulnerability Meldung innerhalb von 72 Stunden, inkl. erster technischer Analyse und Risikobewertung.
- Abschlussbericht innerhalb von 14 Tagen nach Bereitstellung der Abhilfemaßnahme.

Die Meldungen werden über die ENISA Single Reporting Plattform (SRP) und das zuständige nationale CSIRT (CERT-Bund) eingereicht. GROB stellt sicher, dass innerhalb von 14 Tagen entweder eine dauerhafte Abhilfemaßnahme implementiert wird oder eine wirksame risikomindernde Zwischenmaßnahme zur Stabilisierung der Sicherheitslage eingeführt ist.

GROB-WERKE GmbH & Co. KG • Industriestraße 4 • 87719 Mindelheim
+49 (8261) 996-0 • psirt@grob.de

www.grobgroup.com

Cybersecurity@GROB

GROB VULNERABILITY DISCLOSURE GUIDELINE (CVD-PROZESS)

5. Veröffentlichung eines Security Advisories

Nach Bereitstellung einer temporären Risikominderung oder der endgültigen Behebung veröffentlicht GROB ein Security Advisory in Klartextversion sowie in maschinenlesbarer Form.

Das Advisory enthält insbesondere:

- Beschreibung der Schwachstelle, betroffene Produkte und Versionen sowie die Schweregradbewertung
- Empfohlene Gegenmaßnahmen und Hinweise zur Verfügbarkeit von Patches oder Updates

Die Security Advisories werden sowohl als PDF als auch im maschinenlesbaren CSAF 2.0-Format (JSON) veröffentlicht und über die zentrale GROB-Security-Seite einschließlich der zugehörigen CSAF-Provider-Metadaten bereitgestellt.

6. Verantwortungsvolle Offenlegung

GROB verfolgt eine koordinierte Offenlegungspraxis: Sicherheitsmeldungen werden erst veröffentlicht, wenn eine Lösung bereitsteht oder keine unmittelbare Gefahr mehr besteht.

Bei aktiv ausgenutzten Schwachstellen warnt GROB betroffene Nutzer frühzeitig, um Risiken zu minimieren.

3. Datenschutz & Vertraulichkeit

Personenbezogene Daten verarbeiten wir ausschließlich zur Fallbearbeitung gemäß geltenden Datenschutzvorschriften. Veröffentlichungen erfolgen nur mit Ihrer Einwilligung. Vertrauliche Meldungen werden verschlüsselt angenommen und behandelt. Weitere Infos entnehmen Sie bitte unserer Datenschutzerklärung.

GROB-WERKE GmbH & Co. KG • Industriestraße 4 • 87719 Mindelheim
+49 (8261) 996-0 • psirt@grob.de

www.grobgroup.com