CVD-Richtlinie der Thomas GmbH

Revision 1.0 / Autor: Poch, Rube, Brni, Pc

1 Koordinierte Meldung und Offenlegung von Schwachstellen

Die Thomas GmbH, nachfolgend Thomas genannt, nimmt Schwachstellenmeldungen ernst. Wenn Sie eine mögliche Schwachstelle in Produkten, IT-Systemen, Webseiten oder Diensten von Thomas finden, teilen Sie diese bitte verantwortungsvoll mit. Thomas prüft Ihre Meldung, koordiniert die Behebung und informiert über notwendige Maßnahmen.

Ziel dieser Richtlinie ist es, Schwachstellen verantwortungsvoll, vertraulich und koordiniert zu behandeln, Risiken für Nutzer, Kunden, Produkte und Systeme zu reduzieren und geeignete Abhilfemaßnahmen zu ermöglichen.

Am koordinierten Offenlegungsprozess können insbesondere meldende Personen, Thomas als Hersteller beziehungsweise Betreiber, betroffene Dritte sowie zuständige Koordinierungsstellen beteiligt sein.

2 Was kann gemeldet werden?

Sie können mögliche Schwachstellen in Produkten, IT-Systemen, Webseiten oder Diensten melden, die von Thomas hergestellt, bereitgestellt oder betrieben werden. Dazu gehören insbesondere Schwachstellen, die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen können.

Schwachstellen in Produkten, Komponenten, Systemen oder Diensten von Drittanbietern, Dienstleistern oder Lieferanten fallen grundsätzlich nicht in den unmittelbaren Geltungsbereich dieser Richtlinie. Solche Schwachstellen müssen direkt an den jeweiligen Anbieter oder die zuständige Koordinierungsstelle gemeldet werden. Führen Sie keine aktiven Tests durch, wenn unklar ist, ob ein Produkt oder System in den Geltungsbereich fällt; kontaktieren Sie in diesem Fall zunächst Thomas.

Allgemeine Supportanfragen, Funktionswünsche, Fragen zur Produktverfügbarkeit und nicht sicherheitsrelevante Fehler werden über dieses Verfahren nicht bearbeitet. Nutzen Sie dafür die Kontaktmöglichkeiten auf unserer Website.

3 So melden Sie eine Schwachstelle

Bitte nutzen Sie für Ihre Meldung die folgenden Meldeformulare:

- für produktbezogene Schwachstellen https://www.thomas-group.com/de/kontakt/#vulnerability
- für Schwachstellen in IT-Systemen, Webseiten oder Diensten https://www.thomas-group.com/de/kontakt/#security

Alternativ senden Sie produktbezogene Schwachstellen an psirt@thomas-group.com und Schwachstellen in IT-Systemen, Webseiten oder Diensten an csirt@thomas-group.com.

Meldungen können anonym erfolgen. Bitte beachten Sie, dass anonyme Meldungen bei Rückfragen, Nachweisen oder technischen Klärungen nur eingeschränkt oder ggf. nicht bearbeitet werden können.

4 Was Ihre Meldung enthalten sollte

Bitte beschreiben Sie die Schwachstelle so nachvollziehbar wie möglich. Hilfreich sind:

- betroffenes System, Produkt, Komponente, Steuergerät oder Softwaremodul, möglichst mit Bezeichnung, HW-/ SW-Version sowie Seriennummer
- eine kurze Beschreibung der Schwachstelle und Schritte zur Reproduktion
- mögliche Auswirkungen (Vertraulichkeit, Integrität, Verfügbarkeit, Safety- und/ oder Datenschutz-Auswirkung)
- Datum der Entdeckung sowie vorhandene Nachweise wie Proof-of-Concept, Berichte, Logs, Screenshots oder Netzwerkmitschnitte
- ob die Schwachstelle bereits öffentlich bekannt ist oder mit Dritten geteilt wurde (z.B. Verweis auf CVE-Kennungen)

- ob die Schwachstelle bereits aktiv genutzt wird
- sowie Ihre Kontaktdaten für Rückfragen (sofern die Meldung nicht anonym erfolgen soll).

Senden Sie keine personenbezogenen Daten, Passwörter oder vertraulichen Inhalte.

Automatisierte Berichte oder Scan-Ergebnisse sollten nur eingereicht werden, wenn sie einen konkreten Bezug zu einer Schwachstelle haben und ausreichend technisch erläutert sind.

5 Bitte beachten Sie beim Testen

Handeln Sie umsichtig und nur im erforderlichen Umfang. Vermeiden Sie Störungen, Datenveränderungen, unzulässige Zugriffe, Rechteausweitungen, die Veröffentlichung vertraulicher Informationen sowie Tests, die Thomas oder Dritte beeinträchtigen könnten. Greifen Sie nicht auf fremde Daten zu und verändern, kopieren, speichern oder löschen Sie diese nicht. Exploits oder Nachweismethoden dürfen nur eingesetzt werden, soweit dies zur Bestätigung der Schwachstelle erforderlich ist; insbesondere nicht zur Datenkompromittierung oder -exfiltration, zur Einrichtung dauerhaften Zugriffs, zur Rechteausweitung oder zum Zugriff auf weitere Systeme.

Nicht zulässige Testmethoden sind:

- Social Engineering, Phishing oder Täuschung von Mitarbeitenden, Kunden oder Dritten
- physische Angriffe, Manipulationen an Gebäuden, Anlagen, Geräten oder Zutrittskontrollen
- Denial-of-Service-, Last- oder Stresstests sowie Maßnahmen, die Verfügbarkeit, Integrität oder Betrieb beeinträchtigen können
- Spam, Brute-Force-Angriffe, Credential Stuffing oder der Einsatz von Malware
- Zugriff auf, Veränderung, Kopie, Speicherung, Löschung oder Offenlegung von Daten Dritter

Sobald Sie eine Schwachstelle bestätigt haben oder auf sensible Daten stoßen, insbesondere personenbezogene Daten, Finanzinformationen, vertrauliche Informationen oder Geschäftsgeheimnisse, stoppen Sie bitte Ihre Tests, informieren Thomas unverzüglich und legen diese Daten nicht gegenüber Dritten offen.

6 Wie Thomas mit Ihrer Meldung umgeht

Thomas bestätigt den Eingang Ihrer Meldung in angemessener Zeit. Anschließend prüft Thomas die Meldung, bewertet Risiko und Auswirkungen, bindet zuständige Teams ein und plant geeignete Maßnahmen. Darüber setzen wir Sie selbstverständlich in Kenntnis.

Der koordinierte Offenlegungsprozess endet in der Regel, wenn die Meldung unbegründet ist, die Schwachstelle behoben oder angemessen gemindert wurde oder eine Abhilfemaßnahme bereitsteht. Sofern eine Kontaktmöglichkeit vorliegt, informiert Thomas die meldende Person über wesentliche Schritte.

7 Koordinierte Offenlegung von Schwachstellen

Veröffentlichen Sie keine technischen Details, bevor Thomas die Schwachstelle geprüft und angemessene Maßnahmen umgesetzt oder abgestimmt hat. Thomas stimmt Zeitpunkt und Umfang einer Veröffentlichung nach Möglichkeit mit Ihnen, betroffenen Dritten und zuständigen Stellen ab.

8 Umgang mit verantwortungsvollen Meldungen

Wir werden keine rechtlichen Schritte gegen Sicherheitsforscher einleiten, die:

- in gutem Glauben handeln
- diese Richtlinie befolgen
- keine Daten exfiltrieren oder Systeme beschädigen.

Voraussetzung ist, dass Ihre Aktivitäten ausschließlich dem Auffinden, Verifizieren und Melden von Sicherheitslücken dienen und auf das erforderliche Maß beschränkt bleiben. Dies gilt nicht für Handlungen, die über verantwortungsvolle Sicherheitsprüfungen hinausgehen oder gegen geltendes Recht verstoßen. Thomas

kann keine Zusagen für Dritte, insbesondere Kunden, Lieferanten, Dienstleister, Behörden oder andere Rechteinhaber, abgeben.

9 Datenschutz

Vermeiden Sie den Zugriff auf personenbezogene Daten. Falls Sie unbeabsichtigt personenbezogene Daten sehen, speichern, kopieren oder veröffentlichen Sie diese nicht und informieren Sie Thomas unverzüglich.

Thomas verwendet personenbezogene Daten aus Ihrer Meldung nur zur Bearbeitung, Kommunikation und Erfüllung gesetzlicher Pflichten. Weitere Informationen zur Verarbeitung personenbezogener Daten finden Sie in der Datenschutzerklärung von Thomas (www.thomas-group.com/de/datenschutz).