STRATEGIA

情報セキュリティ伴走支援

OSS Vulnerability Report

OSS脆弱性レポート 無料版

加工済み依存関係データと公開脆弱性情報に基づき 顧客回答 開発者確認 監査準備の初動整理に使うための一次調査資料です

本レポートは最終的な安全証明ではありません。 まず何を確認すべきか、どこから人による追加確認が必要かを整理するための資料です。

無料版の範囲

無料版は加工済み依存関係データを公開脆弱性情報と照合し、 顧客回答前に確認すべき候補を自動で一次仕分けする資料です。

- 無料版で扱うもの: package名 version ecosystem scope relationship OSV/GHSA/CVE系ID 先頭IDへのOSVリンク 候補件数 照合対象外理由
- 無料版で断定しないもの: CVSS 重大度 EPSS 悪用状況 修正版候補 本番影響 到達可能性 顧客通知要否
- 顧客提出用の正式文面 監査提出用の証跡整理 開発チケット化 専門家レビューは無料版の範囲外です。

確認目安の読み方

この確認目安は無料レポート内の確認優先度を示すものであり、 最終的な危険度や影響有無を断定するものではありません。

通常

自動照合上 その項目だけを理由に追加確認を強く促す状態ではありません。ただし安全証明ではありません。

要確認

候補あり version不明 private package 照合対象外など 人が確認すべき論点があります。

注意

候補数が多いなど 顧客回答前に優先して確認すべき状態です。

重要

secret候補など 本来送信停止または強い確認が必要な状態です。

1. 全体サマリー

入力dependency件数

0

要確認

照合対象dependency件数

6

脆弱性候補があるdependency件数

4

要確認

脆弱性候補件数

0

一次所見

今回の入力範囲では dependency 情報を確認できませんでした。

入力ファイルの形式 対象プロジェクト 依存関係の記載有無を確認してください。

顧客回答や監査記録として利用するには 依存関係情報を再確認したうえで再生成することを推奨します。

確認上の注意点

- 脆弱性候補があるdependencyが 4 件あります。顧客回答前に優先確認してください。

この章はレポート全体の概要です。 入力データの規模、公開脆弱性情報との照合状況、優先して確認すべき論点をまとめています。

2. 責任者向け要約

責任者向け要約

この無料レポートは 顧客へそのまま提出する最終回答ではなく 顧客回答前に社内で何を確認すべきかを整理する一次資料です。

責任者は この資料を見て 既知脆弱性候補の有無 本番利用確認の必要性 一次回答案として使える範囲を判断してください。

責任者が確認すべき判断ポイント

1. 既知脆弱性候補があるため 顧客回答前に開発者確認と責任者確認を優先してください。
2. この無料レポートを社内確認用資料として扱うか 顧客提出用の文書として整える必要があるか。
3. 既知脆弱性候補があるdependencyについて 開発者が本番利用有無を確認できているか。
4. 確認済み事項と未確認事項を分けて顧客へ説明できるか。
5. 影響なし 対応不要 対応済み などの断定的な表現を使う必要があるか。
6. 顧客に出す前に 責任者が承認できる文面と構成になっているか。

3. 顧客向け一次回答案

以下は顧客へそのまま最終提出する文書ではなく、 確認済み事項と未確認事項を分けるための一次回答のたたき台です。 御社の責任者が内容を確認したうえで調整してください。

> 当社の依存関係情報に基づく一次確認では 現時点で有効なdependency情報を十分に確認できていません。
>
> 対象ファイルまたはSBOMの内容を再確認し 公開OSS名およびversionが確認できる情報をもとに追加調査を行います。
>
> 現時点では影響有無を判断できる材料が不足しているため 追加確認後に改めて回答します。

> [有料]顧客提出用詳細レポート: この一次回答案をもとに 顧客に提出しやすい文面へ整え 確認済み事項 未確認事項 対応予定を分けて記載します。
>
> [有料]専門家レビュー付きレポート: 断定してよい表現 避けるべき表現 契約や監査で誤解されやすい表現を確認します。

4. 開発者向け確認事項

顧客回答前に開発チームまたはシステム責任者へ確認すべき項目です。

1. 既知脆弱性候補があるdependencyを優先して確認してください。
2. 対象dependencyが本番ビルドまたは本番実行環境に含まれるか確認してください。
3. 対象dependencyが本番環境で使われる可能性がある依存関係か 開発やテストだけで使う依存関係かを確認してください。
4. 脆弱性が成立する機能やコードパスを実際に利用しているか確認してください。
5. 外部ユーザーまたは認証前ユーザーから問題箇所まで実際に届く可能性があるか確認してください。
6. 修正版または回避策が存在する場合は 更新可否 影響範囲 回帰テスト範囲を確認してください。
7. 顧客回答前に 確認済み事項 未確認事項 対応予定を分けて整理してください。

> [有料]顧客提出用詳細レポート: この確認事項を開発チームへ依頼しやすい確認項目やチケット文面へ整理し顧客回答へ反映しやすくします。
>
> [有料]専門家レビュー付きレポート: RCE 認証前到達 外部公開機能への影響など 自動処理だけで判断しにくい論点を確認します。

5. 入力データ概要

入力種別	cyclonedx
dependency件数bucket	1_50
private package件数bucket	1_10
URL削除件数bucket	1_10
secret候補検出	検出なし

ecosystem別件数

分類	件数	確認目安
npm	9	通常

scope別件数

分類	件数	確認目安
runtime	7	通常
optional	2	通常

relationship別件数

分類	件数	確認目安
unknown	9	通常

照合可否分類

分類	件数	確認目安
queryable	6	通常
private	3	要確認

> [有料]顧客提出用詳細レポート: version不明 private package 照合対象外の範囲を 顧客へ説明できる形に整理します。
>
> [有料]専門家レビュー付きレポート: 入力データの不足がリスク判断や顧客説明にどの程度影響するかを確認します。

6. 公開脆弱性照合結果サマリー

この章は1章の全体サマリーのうち、公開脆弱性情報との照合結果だけを切り出した内訳です。 入力データ全体の説明ではなく、既知脆弱性候補と照合対象外の理由を確認するための章です。

照合対象dependency件数	6
脆弱性候補があるdependency件数	4
脆弱性候補件数	0

照合対象外の理由別件数

該当データはありません

> [有料]顧客提出用詳細レポート: 脆弱性候補ごとに 顧客回答で触れるべき項目 社内確認に留める項目 対応予定を整理します。
>
> [有料]専門家レビュー付きレポート: 重要度が高い候補や判断が難しい候補について 人による影響観点の確認を加えます。

7. 優先確認項目

優先確認項目は、脆弱性候補数が多いものを先にし、同数の場合は本番利用されやすいscope、直接依存、package名の順に表示しています。 重大度 悪用状況 修正版の有無そのものの順序ではありません。 無料版ではOSV ID列のOSVリンクは先頭1件だけです。2件目以降はIDのみ表示します。

既知脆弱性候補が検出された照合対象dependencyはありません。

ただし version unknown や private package や未対応ecosystem は照合対象外です。

> [有料]顧客提出用詳細レポート: 優先確認候補を 顧客回答上の優先度 開発対応上の優先度 監査証跡上の優先度 に分けて整理します。
>
> [有料]専門家レビュー付きレポート: 高リスク候補について 修正を急ぐべきか 追加調査が必要か 顧客へ先に説明すべきかを確認します。

8. 監査・委託先審査向けの記録

監査や委託先審査では、検知したことだけでなく、 検知後にどのように整理し、何を未確認として残したかを説明できることが重要です。 ここでは脆弱性対応の判断記録として使いやすい項目だけを記載します。

調査種別	加工済み依存関係データに基づくOSS脆弱性一次調査
入力データ種別	cyclonedx
入力dependency件数	0
公開脆弱性情報との照合対象件数	6
脆弱性候補があるdependency件数	4
脆弱性候補件数	0
照合対象外の主な理由	特記なし
追加確認が必要な代表項目	本番利用有無 該当機能の利用有無 外部到達可能性 修正版適用可否 顧客通知要否

> [有料]顧客提出用詳細レポート: 検知後に何を確認し 何を未確認として残したかを 監査や委託先審査で説明しやすい記録へ整えます。
>
> [有料]専門家レビュー付きレポート: 監査人や顧客が疑問に持ちやすい論点と 不足している証跡を確認します。

9. レポート生成条件とデータ取扱い

以下は監査判断そのものではなく、この無料レポートを作成するための入力条件とデータ取扱いに関する情報です。

生ファイル送信	送信していません
private package名	匿名化または件数化しています
secret候補	検出なし
人による個別確認	無料レポート範囲には含みません
生成方式	提供された加工済み依存関係データと公開脆弱性情報に基づく自動生成

10. 免責・注意事項

ストラテジアの責任範囲について

本レポートは 利用者が提供した加工済み依存関係データと公開脆弱性情報をもとに自動生成した参考資料です。

株式会社ストラテジアは 本レポートの内容をもって 入力データの完全性 公開脆弱性情報の網羅性 実環境での影響有無 顧客提出の適否 契約上または法令上の通知要否を保証しません。

本レポートは脆弱性診断 侵入テスト ソースコードレビュー 到達可能性解析 法的判断 契約判断を代替するものではありません。

最終的な影響判断 顧客提出 リスク受容 修正方針 顧客通知の要否は 利用企業の責任で確認してください。

無料レポートでは ストラテジア担当者による個別確認 専門家レビュー 顧客提出文書としての保証は含みません。

- 本レポートは提供された加工済み依存関係データと公開脆弱性情報に基づく自動生成の一次調査資料です
- 本レポートは脆弱性診断 侵入テスト ソースコードレビュー 到達可能性解析 契約上または法令上の通知義務判断を代替しません
- 本レポートはCVSS 重大度 EPSS 悪用状況 修正版候補 本番影響 顧客通知要否を断定しません
- 本レポートは入力データの完全性 依存関係解決の完全性 公開脆弱性情報の網羅性 実環境における影響有無を保証しません
- version unknown の依存関係は既知脆弱性照合の精度が限定されます
- private package は公開脆弱性情報との照合対象外です
- 最終的な影響判断 顧客提出 リスク受容 修正方針の確定は利用企業の責任で確認してください
- 株式会社ストラテジアは無料レポートの内容について個別確認 専門家レビュー 顧客提出文書としての保証を行いません

発行管理用情報

この情報はレポートの再確認や問い合わせ時の照合に使うための管理情報です。 レポート本文の判断内容そのものではありません。

Report ID	rpt_20260526155451_46e252daf044707c
生成日時	2026-05-26T06:54:55.035Z
入力種別	cyclonedx