OSS脆弱性レポート

STRATEGIA
情報セキュリティ伴走支援

エビデンス

根拠を揃えるために、加工済みOSS部品データ、公開脆弱性情報、サーバ側で確定した管理情報をもとに、自動照合で得た候補IDと根拠を全量整理します。

本資料は、お客様へ回答する前に、社内で確認内容を整理するための資料です。

公開脆弱性ID候補は、利用箇所・到達性・更新可否等を人が確認するための入口です。重大度や最終的な安全判断を表すものではありません。

レポートの読み方

本レポートでは、自動照合で見えた事実、見えていない範囲、次に人が確認すべき論点を分けて示します。候補が表示されている場合でも、影響有無や通知要否を断定する資料ではありません。

読む順番	確認すること	扱い
サマリ	入力規模、照合範囲、公開脆弱性ID候補数	初動の全体像として扱います
対象範囲・制約	照合できた範囲と限界	不足情報の追記対象として扱います
優先確認	候補ID、OSS部品、依存関係の種類	人が確認する入口として扱います
次の確認	担当者、期限、追加調査	実際の対応計画に写します

凡例 / バッジの見方

バッジ	このレポートでの扱い
候補あり	公開脆弱性ID候補があり、人が確認する入口として扱います
照合済み	公開情報との照合結果を記録済みとして扱います
追加確認	照合に必要な情報や利用状況を追加で確認する対象として扱います
照合対象外	公開情報と自動照合しない範囲として扱います
初動確認	自動照合だけで製品影響を判断せず、利用箇所・到達性・更新可否等を人が確認する対象です。重大度ではありません。

各バッジは自動照合結果を読みやすくするための表示です。CVSS、EPSS、悪用可能性、修正版の有無、顧客通知要否を確定するものではありません。

1. エグゼクティブサマリ

入力OSS部品件数

8

照合済み

今回扱ったOSS部品の規模です

公開情報と照合可能なOSS部品件数

6

追加確認

公開脆弱性情報と自動照合できた範囲です

候補ありOSS部品件数

3

候補あり

公開脆弱性ID候補数

9

候補あり

公開脆弱性ID候補がひも付いたOSS部品です	ID単位。同一脆弱性に複数識別子の場合あり

候補が0件の場合は「候補なし。ただし安全性の証明ではない」と扱います。候補がある場合も、影響あり・影響なし・顧客通知要否をこの資料だけで断定しません。

2. 入力範囲・照合範囲

項目	値
入力種別	cyclonedx
入力OSS部品件数の範囲	1_50
非公開OSS部品件数の範囲	1_10
URL削除件数の範囲	0
secret候補検出	なし

パッケージ種別別件数

分類	件数
npm	7
unknown	1

利用区分別件数

分類	件数
任意	2
利用区分不明	6

依存関係の種類別件数

分類	件数
利用関係不明	8

照合可否分類

分類	件数
非公開OSS部品	1
公開情報と照合可能	6
バージョン不明	1

3. OSS部品台帳

この台帳は入力から得たOSS部品を、パッケージ種別、利用区分、依存関係の種類、公開脆弱性ID候補数で整理します。公開脆弱性IDの全量は付録へ集約します。

OSS部品	バージョン	パッケージ種別	利用区分	依存関係の種類	公開脆弱性ID候補数
private:sample:001	1.0.0	unknown	任意	利用関係不明	0
zod	3.23.8	npm	任意	利用関係不明	0
webpack-dev-server	3.11.2	npm	利用区分不明	利用関係不明	6
node-fetch	2.6.0	npm	利用区分不明	利用関係不明	2
json5	1.0.1	npm	利用区分不明	利用関係不明	1
left-pad	unknown	npm	利用区分不明	利用関係不明	0
picocolors	1.1.1	npm	利用区分不明	利用関係不明	0
react	18.2.0	npm	利用区分不明	利用関係不明	0

4. 優先確認候補

確認順は、公開脆弱性ID候補数、実行時依存、直接依存、OSS部品名の順で整理します。これは確認開始の順番であり、CVSS、EPSS、悪用状況、修正版の有無、顧客通知要否の順番ではありません。

OSS部品	バージョン	パッケージ種別	利用区分	依存関係の種類	公開脆弱性ID候補数	初動
webpack-dev-server	3.11.2	npm	利用区分不明	利用関係不明	6	初動確認
node-fetch	2.6.0	npm	利用区分不明	利用関係不明	2	初動確認
json5	1.0.1	npm	利用区分不明	利用関係不明	1	初動確認

5. 主張境界台帳

主張	状態	根拠・境界
自動照合で得た候補IDと根拠を整理	確認済み	公開情報との自動照合で得た根拠
顧客回答前の社内確認材料	確認済み	顧客回答文は生成しない
生成AIへ送信しない	確認済み	生成AIへ送信しない
製品影響・到達性・更新可否・顧客通知要否は未確認	未確認	利用箇所、到達性、修正版適用可否、対外通知判断

主張	状態	根拠・境界
初動確認	追加確認	実利用箇所と到達可能性を確認

6. 開発者確認票

OSS部品	確認対象	次に確認すること	確認結果
webpack-dev-server 3.11.2	利用箇所と到達可能性を確認	直接依存か間接依存か、上位依存関係を確認	未確認
node-fetch 2.6.0	利用箇所と到達可能性を確認	直接依存か間接依存か、上位依存関係を確認	未確認
json5 1.0.1	利用箇所と到達可能性を確認	直接依存か間接依存か、上位依存関係を確認	未確認

7. 対応管理表

OSS部品	担当者	期限	状態	確認結果
webpack-dev-server 3.11.2	未設定	未設定	追加確認	直接依存か間接依存か、上位依存関係を確認
node-fetch 2.6.0	未設定	未設定	追加確認	直接依存か間接依存か、上位依存関係を確認
json5 1.0.1	未設定	未設定	追加確認	直接依存か間接依存か、上位依存関係を確認

8. 監査・委託先審査で説明を準備するための記録

記録項目	値	扱い
監査・委託先審査で説明を準備するための記録	確認済み	顧客回答前の社内確認材料
OSS部品	8	入力種別とOSS部品件数範囲を確認済み
公開情報と照合可能	6	公開情報と照合可能なOSS部品数を確認済み
公開脆弱性ID候補数	9	ID単位。同一脆弱性に複数識別子の場合あり
照合対象外	追加確認	照合対象外または追加確認の理由を件数で記録

対象範囲・制約

- 本レポートは提供された加工済みOSS部品データと公開脆弱性情報に基づく自動生成資料です。
- 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、実環境影響、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。
- バージョン不明のOSS部品は既知脆弱性照合の精度が限定されます。
- 非公開OSS部品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、対外回答、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。

共通ノート

- 本レポートは エビデンス として生成され、役割は「根拠を揃える」です。
- 成果物の保持期間は 14日 です。
- 提供状態は 提供中 です。
- 公開脆弱性IDのリンク方針は本資料の種類ごとに固定され、入力内容からは変更しません。

作成時情報の見方

この情報は、レポートID、JST生成日時、表示版を後続確認で照合するための記録です。HTMLとPDFの同一性確認、保管期限の確認、再生成時の差分確認の起点として扱います。

項目	値
レポートID	rpt_20260823_204128_IkZ1
生成日時	2026年8月23日 20:41 JST
入力種別	cyclonedx
保存期間	14日
テンプレートバージョン	26081902

付録. 公開脆弱性ID台帳

この付録は、表示する有効な公開脆弱性IDを1箇所に統合した台帳です。各IDはosv.devの公開情報へリンクします。

OSS部品	バージョン	パッケージ種別	公開脆弱性ID	扱い
webpack-dev-server	3.11.2	npm	GHSA-4v9v-hfq4-rm2v	ID単位。同一脆弱性に複数識別子の場合あり
webpack-dev-server	3.11.2	npm	GHSA-79cf-xcqc-c78w	ID単位。同一脆弱性に複数識別子の場合あり
webpack-dev-server	3.11.2	npm	GHSA-9jgg-88mc-972h	ID単位。同一脆弱性に複数識別子の場合あり
webpack-dev-server	3.11.2	npm	GHSA-f5vj-f2hx-8m93	ID単位。同一脆弱性に複数識別子の場合あり

OSS部品	バージョン	パッケージ種別	公開脆弱性ID	扱い
webpack-dev-server	3.11.2	npm	GHSA-m28w-2pqf-7qgj	ID単位。同一脆弱性に複数識別子の場合あり
webpack-dev-server	3.11.2	npm	GHSA-mx8g-39q3-5c79	ID単位。同一脆弱性に複数識別子の場合あり
node-fetch	2.6.0	npm	GHSA-r683-j2x4-v87g	ID単位。同一脆弱性に複数識別子の場合あり
node-fetch	2.6.0	npm	GHSA-w7rc-rwvf-8q5r	ID単位。同一脆弱性に複数識別子の場合あり
json5	1.0.1	npm	GHSA-9c47-m6qq-7p4h	ID単位。同一脆弱性に複数識別子の場合あり