

EXECUTIVE SUMMARY

Webサイト脆弱性診断結果報告書

本報告書は、SiteHoundによる非破壊診断の結果をまとめたものです。攻撃による侵入の実証は行わず、サーバ応答からのバージョン特定と既知脆弱性（NVD / CISA KEV）の照合にとどめています。

TARGET https://example.com

SCANNED 2026-10-20 14:32

MODE 非破壊 / 6ページ巡回

DURATION 48秒

RISK SCORE

6.2/10

GRADE C

0 5 10

要即時対応が1件。公開されたままのバックアップと、既知の悪用済み脆弱性が該当します。

FINDINGS BY SEVERITY

■ 要即時対応	1
■ 要対応	2
■ 参考	5

検出8件のうち、CISA KEV（実際に悪用が確認された脆弱性）に該当するものは1件です。

PAGES

6 ページ

CVE MATCH

14 件

KEV

1 件

EXPOSED

2 件

SCORE

6.2/10

まず、この2つから。

① Apache HTTP Server 2.4.49（CVE-2021-41773）。実際に悪用が確認されているパストラバーサル脆弱性です。バージョンアップを最優先してください。② /backup/site-2024.zip が認証なしで取得できる状態です。ソースコードや設定が含まれている場合、情報漏洩に直結します。公開ディレクトリからの移動、またはアクセス制限をかけてください。残る6件は、次回の定期診断までに順次対応いただければ十分です。

FINDINGS

検出された指摘と、直す順番

検出8件を、実際の悪用リスクの高い順に並べています。CVSSはNVDのスコア、KEVは実際に悪用が確認された脆弱性であることを示します。

指摘	区分	CVSS	内容
Apache HTTP Server 2.4.49 CVE-2021-41773 / PATH TRAVERSAL	要即時対応 KEV	7.5	パス正規化の不備により、公開ディレクトリ外のファイルが読まれる可能性があります。実際に悪用が確認されています。 2.4.51以降へ更新 してください。
/backup/site-2024.zip EXPOSED FILE / 200 OK	要即時対応	—	認証なしで取得できる状態です。ソースや設定が含まれる場合、情報漏洩に直結します。公開領域から退避し、アクセス制限をかけてください。
jQuery 1.12.4 CVE-2015-9251 / XSS	要対応	6.1	クロスサイトスクリプティングの既知脆弱性を含む旧版です。3.x系への更新、または該当機能の置き換えを。
PHP 7.4.33 END OF LIFE	要対応	—	サポートが終了しており、今後判明する脆弱性の修正が提供されません。8.x系への移行計画を立ててください。
X-Powered-By ヘッダ INFORMATION DISCLOSURE	参考	—	サーバソフトウェア名が応答に含まれています。攻撃の足がかりになり得るため、非表示を推奨します。
TLS 1.0 / 1.1 有効 WEAK PROTOCOL	参考	—	古いTLSが有効です。TLS 1.2以上に限定し、暗号スイートも見直してください。

STEP 01 / 今週

Apache の更新

要即時対応の1件。更新後、SiteHoundで再診断し、差分が消えたことを確認します。

STEP 02 / 今月中

バックアップの退避

公開領域から移動。併せて、公開されているファイルの棚卸しを行います。

STEP 03 / 次回まで

ライブラリとヘッダ

jQuery・PHPの更新計画を立て、ヘッダ類の情報露出を削ります。

STANCE / 診断の姿勢

本診断は、攻撃による侵入の実証を行いません。対象サイトのバージョン特定と既知脆弱性の照合にとどめ、同一ホストの範囲を出ません。診断は対象サイトの所有者、または許可を得たうえで実施します。認証情報は保存しません。本レポートはサンプルであり、example.com は実在のサイトではありません。