PentaTrail

対処ガイダンスレポート 見本 / SAMPLE

対象ドメイン example.co.jp · 生成日 2026-07-06 · 並び 脅威エクスポージャーリスク（TER）が高い順

この資料は架空企業「サンプル商事株式会社」のデータで作成した見本です。実在の企業・組織とは関係ありません。

AI 改善ガイダンスの要約

S 2件 | A 2件 | B 2件 | C 1件

重要度の凡例: S A B C D

S Apache HTTP Server 2.4.49

対象ホスト 2 · CVE 2

影響

経路の正規化に不備があり、公開ディレクトリの外にあるファイルへ到達できます。設定によっては、サーバ上のプログラムを外部から実行される場合があります。既に悪用が確認されている部品です。

対処方針

2.4.51 以降へ更新してください。ディストリビューションの配布版を使っている場合は、該当のパッチが取り込まれた版へ上げれば同じ効果があります。更新後は Apache の再起動が必要です。

暫定緩和策

すぐに更新できない場合は、設定ファイルの Directory ディレクティブで「/」に対する Require all denied を明示し、公開する範囲だけを個別に許可してください。

紐づく CVE

CVE-2021-41773 CVE-2021-42013

対象ホスト（2）

www.example.co.jp shop.example.co.jp

S OpenSSL 3.0.0

対象ホスト 1 · CVE 2

影響

証明書に含まれる文字列の処理でバッファの範囲を超えて書き込む不具合があり、クライアント証明書を受け付ける構成では、接続してきた相手から動作を乱される可能性があります。

対処方針

3.0.7 以降へ更新してください。更新後、OpenSSL を静的に取り込んでいるアプリケーションは再ビルドが必要です。

暫定緩和策

クライアント証明書による認証を一時的に無効にすると、この経路からの影響は受けなくなります。

紐づく CVE

CVE-2022-3602 CVE-2022-3786

対象ホスト（1）

vpn.example.co.jp

A PHP 7.4.x（サポート終了）

対象ホスト 1 · CVE 1

影響

サポートが終了しており、今後の不具合に対する修正が提供されません。過去には、特定の構成で外部から任意のコードを実行できる不具合が見つかっています。

対処方針

PHP 8.2 以降へ移行してください。移行時は、非推奨になった関数の置き換えと、型の扱いが厳しくなった箇所の確認が必要です。

紐づく CVE
CVE-2019-11043

対象ホスト（1）
api.example.co.jp

A nginx 1.18.0

対象ホスト 2 · CVE 1

影響
名前解決の応答を処理する部分に不具合があり、上流の名前解決を経由する構成では、細工された応答によって動作を乱される可能性があります。

対処方針
1.20.1 以降へ更新してください。設定の変更は不要です。

暫定緩和策
設定内で resolver ディレクティブを使っていない場合、この経路は成立しません。使っている場合は、信頼できる名前解決先だけを指定してください。

紐づく CVE
CVE-2021-23017

対象ホスト（2）
www.example.co.jp
api.example.co.jp

B 送信ドメイン認証の未設定

対象ホスト 1

影響
このドメインを差出人に用いたメールが本物かどうかを、受信側が判定できません。取引先を装ったメールに使われる余地が残ります。

対処方針
SPF レコードを設定し、送信に使うサーバだけを許可してください。あわせて DMARC を p=none で導入し、実際の送信状況を集計してから段階的に強めることをおすすめします。

対象ホスト（1）
mail.example.co.jp

B TLS 証明書のホスト名不一致

対象ホスト 1

影響
提示している証明書の名前が、接続先のホスト名と一致していません。利用者のブラウザに警告が出るほか、警告に慣れてしまうと、本物と偽物の区別がつかなくなります。

対処方針
このホスト名を含む証明書を発行し直して差し替えてください。複数の名前で受けている場合は、すべての名前を証明書に含めてください。

対象ホスト（1）
shop.example.co.jp

C セキュリティヘッダーの不足

対象ホスト 2

影響
ブラウザ側の防御を有効にするヘッダーが出ていません。単独で被害につながるものではありませんが、別の不具合と重なったときに影響が広がりやすくなります。

対処方針

Content-Security-Policy と X-Content-Type-Options を設定してください。Content-Security-Policy は最初に Report-Only で入れ、既存の表示が壊れないことを確かめてから有効にします。

対象ホスト（2）

example.co.jp www.example.co.jp