脆弱性診断レポート

会社名：	株式会社 XXXXX
診断対象サイト：	www.xxxxxx.co.jp
診断日：	2023年xx月xx日

一般社団法人
中小企業サイバーセキュリティ支援協会

目　次

1．エグゼクティブサマリ

◆対象ドメイン

skyjapan.co.jp

◆診断日

2021年10月1日実施

◆診断結果

Critical	（緊急）	・・・	3 件
High	（高い）	・・・	8 件
Medium	（普通）	・・・	15 件
Low	（低い）	・・・	2 件
Info	（情報）	・・・	58 件

◆考察

今回の脆弱性診断の結果、「Critical（緊急）」が３件、「High（高い）」が８件あり、すぐに対策をする必要があります。
一つ一つの脆弱性結果詳細を確認の上、推奨対策を上げておりますので、それを参照に対策をしてください。

3. 脆弱性一覧

	リスク度	CVSS V3.0	脆弱性内容	Plugin ID
1	Critical	7.5	7.2 より前の OpenSSH における信頼できない X11 転送フォールバックのセキュリティバイパス	90022
2	Critical	10.0	Unixオペレーティングシステムでサポートされていないバージョンの検出	33850
3	Critical	10.0	WordPressでサポートされていないバージョンの検出	84019
4	High	8.5	6.9より前の OpenSSHにおける複数の脆弱性	84638
5	High	7.8	スクリプトSrc整合性チェック	119811
6	High	7.5	6.6より前の OpenSSHにおける複数の脆弱性	73079
7	High	7.5	7.4より前の OpenSSHにおける複数の脆弱性	96151
8	High	7.2	7.3より前の OpenSSHにおける複数の脆弱性	93194
9	High	6.5	4.9.9より前のWordPressにおけるリモートコード実行の脆弱性	125597
10	High	5.0	ProFTPD <1.3.5b / 1.3.6x <1.3.6rc2弱いDiffie-Hellman鍵	106755
11	High	10.0	MTAオープンメールリレーが許可されました	10262
12	Medium	8.5	7.0より前の OpenSSHにおける複数の脆弱性	85382
13	Medium	6.1	TLSバージョン1.0プロトコル検出	104743
14	Medium	5.8	HTTPSサーバーからHSTSが欠落している（RFC 6797）	142960
15	Medium	5.5	7.2p2 より前の OpenSSH における X11Forwarding xauth コマンドインジェクション	90023
16	Medium	5.0	OpenSSH <7.5	99359

４－１．Critical脆弱性の詳細

４－１－１．

リスク度	CVSS V3.0	脆弱性内容	Plugin ID
Critical	7.5	7.2 より前の OpenSSH における信頼できない X11 転送フォールバックのセキュリティバイパス	90022

【概要】

リモートホストで実行されている SSH サーバーは、セキュリティバイパスの脆弱性の影響を受けます。

【説明】

バナーによると、リモートホストで実行している OpenSSH のバージョンは、7.2 より前です。このため、セキュリティバイパスの脆弱性の影響を受けます。この原因は、SECURITY 拡張機能が X サーバーにより無効にされている場合、ssh(1) が信頼できない X11 転送から信頼できる転送にフォールバックする際に、誘発される欠陥があるためです。これにより、X11 接続は、リモートの攻撃者により悪用される可能性があるため、信頼できないものになる可能性があります。

【推奨事項】

OpenSSH バージョン 7.2 または以降にアップグレードしてください。

【参照CVE】

CVE-2016-1908

【関連情報】

http://www.openssh.com/txt/release-7.2

４－２．High脆弱性の詳細

４－２－２．

リスク度	CVSS V3.0	脆弱性内容	Plugin ID
High	7.8	スクリプトSrc整合性チェック	119811

【概要】

整合性を使用していない外部スクリプトリソースを報告します。

【説明】

リモートホストは、信頼できない可能性があり、検証されていないサードパーティのスクリプトsrcからJavaScriptが含まれているため、支払いエントリデータの漏えいに対して脆弱である可能性があります。
ホストがサードパーティによって制御されている場合は、サードパーティがPCIDSSに準拠していることを確認してください。

【推奨事項】

ターゲットスクリプトにスクリプト整合性チェックを設定するか、ターゲットスクリプトを削除します。

【参照CVE】

【関連情報】

http://www.nessus.org/u?c9e76c4f
https://www.w3.org/TR/SRI/
http://www.nessus.org/u?f39144f8