SSH インスペクタ

SSH インスペクタの概要

タイプ	インスペクタ（サービス）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	なし
有効	`true`

Secure Shell Protocol （SSH）は、セキュリティで保護されていないネットワークを介したクライアントとサーバー間の安全な通信を可能にするネットワークプロトコルです。SSHはトンネリングをサポートし、公開鍵暗号化を使用してリモートホストを認証します。

SSHを使用してファイルを安全に転送したり、リモートホストにログインしてコマンドラインと連携動作したりできます。SSHプロトコルは、TCP、UDP、またはSCTPを介してポート22を使用します。

`ssh` インスペクタは、ストリームパケットを復号化し、次のSSHエクスプロイトを検出します。

- チャレンジ/応答バッファ オーバーフロー エクスプロイト
- CRC-32 エクスプロイト
- SecureCRT SSH クライアント バッファ オーバーフロー エクスプロイト

- 正しくない SSH メッセージの方向

ホスト間のネットワーク接続が暗号化されている場合、認証後にチャレンジ/レスポンス バッファ オーバーフローと CRC-32 攻撃が発生します。どちらのタイプの攻撃も、認証チャレンジ直後に 20 KB を超える大きなペイロードをサーバーに送信します。

ssh インスペクタは、サーバーに送信されたバイト数をカウントすることで、チャレンジ/応答バッファ オーバーフローと CRC-32 攻撃を検出します。バイト数が、事前に定義したパケット数内で定義した制限を超えた場合、ssh インスペクタはアラートを生成します。CRC-32 攻撃の対象となるのは SSH バージョン 1 のみであり、チャレンジ/応答バッファ オーバーフロー エクスプロイトの対象となるのは SSH バージョン 2 のみです。ssh インスペクタは、セッションの開始時に SSH バージョン文字列を読み取り、攻撃のタイプを識別します。

SecureCRT SSH クライアント バッファ オーバーフロー攻撃とプロトコル不一致攻撃は、キー交換前にホストが接続をセキュリティで保護しようとするときに発生します。SecureCRT SSH クライアント バッファ オーバーフロー攻撃では、非常に長いプロトコル識別子の文字列がクライアントに送信され、それが原因でバッファオーバーフローが発生します。プロトコル不一致攻撃は、SSH 以外のクライアント アプリケーションがセキュア SSH サーバーに接続しようとするか、またはサーバーとクライアントのバージョン番号が一致しない場合に発生します。

（注） ssh インスペクタはブロートフォース攻撃を処理しません。

SSH インスペクタを設定するためのベストプラクティス

デフォルトの ssh インスペクタ設定を使用することをお勧めします。max_encrypted_packets パラメータで定義されているセッションの暗号化パケットの最大数を超えると、ssh インスペクタはそのセッションのトラフィックの処理を停止してパフォーマンスを向上させます。ssh インスペクタは、SSH セッションの開始時に表示される SSH の脆弱性のみを検出します。

（注） ssh インスペクタがチャレンジ/応答 オーバーフローまたは CRC 32 で誤検知を生成した場合、max_client_bytes パラメータを使用して、必要なクライアントバイト数を増やすことができます。

SSH インスペクタのパラメータ

SSH サービスの設定

binder インスペクタは、SSH サービスの設定を定義します。詳細については、『バインダインスペクタの概要』を参照してください。

例：

```
[
    {
        "when": {
            "service": "ssh",
            "role": any
        },
        "use": {
            "type": "ssh"
        }
    }
]
```

max_encrypted_packets

ssh インスペクタが SSH セッションを無視するまでに調べる暗号化パケットの最大数を指定します。セッションの暗号化パケットの最大数を超えた場合、パフォーマンスを向上させるために、ssh インスペクタはそのセッションのトラフィックの処理を停止します。

型：整数

有効な範囲：-1 ～ 65535

デフォルト値：25

max_client_bytes

チャレンジ/応答オーバーフローまたは CRC 32 で ssh インスペクタがアラートを生成するまでにサーバーに送信する未応答バイトの最大数を指定します。max_encrypted_packets が送信される前に max_client_bytes の制限を超えた場合、インスペクタは攻撃が発生したと見なし、トラフィックを無視します。

ルール 128:1 を有効にして、インスペクタがチャレンジ/応答オーバーフローを検出したときにアラートを生成するか、ルール 128:2 を有効にして、が CRC 32 エクスプロイトを検出したときにアラートを生成することができます。

クライアントがサーバーから受信する有効な応答ごとに、ssh インスペクタは max_client bytes のパケット数をリセットします。

（注） max_client_bytes を 0 または 1 に設定することはお勧めしません。max_client_bytes を 0 または 1 に設定すると、ssh インスペクタは常にアラートを生成します。

型：整数

有効な範囲：0 ～ 65535

デフォルト値：19600

max_server_version_len

SSH サーバーのバージョン文字列の最大長を指定します。SSH サーバーのバージョン文字列の長さが max_server_version_len を超える場合、ssh インスペクタはアラートを生成します。ルール 128:3 を有効にして、セキュア CRT サーバーのバージョン文字列のオーバーフローのアラートを生成できます。

型：整数

有効な範囲：0 ～ 255

デフォルト値：80

（注） ssh インスペクタのデフォルト設定では、アラートは有効になりません。

SSH インスペクタのルール

ssh インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。 。

表 *1: SSH* インスペクタのルール

GID:SID	ルール メッセージ
128:1	challenge-response オーバーフローのエクスプロイト（challenge-response overflow exploit）
128:2	SSH1 CRC32 エクスプロイト（SSH1 CRC32 exploit）
128:3	サーバーバージョン文字列のオーバーフロー（server version string overflow）
128:5	不正なメッセージの方向（bad message direction）
128:6	指定のペイロードに対してペイロードサイズが正しくない（payload size incorrect for the given payload）
128:7	SSH バージョンの文字列の検出に失敗した（failed to detect SSH version string）

SSH インスペクタの侵入ルールのオプション

ssh インスペクタには、侵入ルールのオプションはありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。