CONFIDENCIAL

SingleID 御中

SingleID Health for CheckPoint
結果報告書

Single ID

2022年2月1日9:15

SingleID

1.目次

2.はじめに

本報告書は、 「2022年2月1日9:07～2022年2月1日9:15」 に実施した脆弱性検査の検査結果についてご報告するものです。

2.1 目的

本検査の目的は、検査対象システムに対してリモートから脆弱性の検査を行い、システムに存在する脆弱性を検出することにあります。 また、脆弱性が検出された場合、そのリスク評価、及び、脆弱性への対策を支援する情報の提供も行います。

3.概要

3.1 検査情報

検査カテゴリ	Basic Network Scan
検査ID	3
検査対象	IP : x.x.x.x Host : x.x.x.x
検査実施日時	2022年2月1日9:07～2022年2月1日9:15

3.2 検査方法

業界トップクラスの広範囲な脆弱性情報を活用し、インターネット経由で、検査対象をリモート診断しました。

3.3 対象者

本報告書は、システムおよびアプリケーション管理者、セキュリティスペシャリスト、監査人、ヘルプデスク、プラットフォームデプロイメント、DevOps担当者を対象としています。

4.検査結果

4.1 ダッシュボード

検査実施日時
2022年2月1日9:07～2022年2月1日9:15
検査対象
IP : x.x.x.x Host : x.x.x.x
検査名
Basic Network Scan

総合　B　判定

直接的に被害を受ける可能性は低いと推測されますが、脆弱性が確認されております。
検出内容を確認の上、対策の検討を行うことを推奨します。

インターネットからアクセス可能な通信ポートごとの診断結果

危険度	重大	高	中	低	情報
22/tcp	0	0	0	1	6

注意

意図しない「インターネットからアクセス可能な通信ポート」が検出されている場合には、機器の設定を見直してください。
特に、ネットワーク機器（ルータ、スイッチ、WiFiアクセスポイント）およびファイアウォール製品の管理コンソール（Web管理GUI、SSH、Telnetなど）を接続元のIPアドレスを制限せずに、インターネットに公開することは推奨されません。

4.2 結果一覧

4.2.1 X.X.X.X

No	検査項目	対象ポート	レベル
1	SSHサーバーのCBCモード暗号が有効	22/tcp	低
2	SSHパスワード認証が受け入れられました	22/tcp	情報
3	SSH SHA-1HMACアルゴリズムが有効	22/tcp	情報
4	サポートされているSSHのアルゴリズムおよび言語	22/tcp	情報
5	SSHサーバーのタイプとバージョン情報	22/tcp	情報
6	サービス検出	22/tcp	情報
7	SYNスキャナー	22/tcp	情報

4.3 結果詳細

4.3.1

危険度	低
検査項目	SSHサーバーのCBCモード暗号が有効
対象ポート	22/tcp
説明	SSHサーバーは、Cipher Block Chaining（CBC）暗号化をサポートするように構成されています。これにより、攻撃者は暗号文から平文メッセージを回復できる可能性があります。 このプラグインはSSHサーバーのオプションのみをチェックし、脆弱なソフトウェアバージョンはチェックしないことに注意してください。
対策	ベンダーに連絡するか、製品のドキュメントを参照して、CBCモードの暗号化暗号化を無効にし、CTRまたはGCM暗号化モードの暗号化を有効にしてください。
出力	The following client-to-server Cipher Block Chaining (CBC) algorithms are supported : aes128-cbc aes256-cbc The following server-to-client Cipher Block Chaining (CBC) algorithms are supported : aes128-cbc aes256-cbc
VPR	2.5
CVSS v2	2.6（CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N）
CVSS v3	
CVE識別番号	CVE-2008-5161

4.3.2

危険度	情報
検査項目	SSHパスワード認証が受け入れられました
対象ポート	22/tcp
説明	リモートホスト上のSSHサーバーはパスワード認証を受け入れます。
対策	該当なし
出力	
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.3

危険度	情報
検査項目	SSH SHA-1HMACアルゴリズムが有効
対象ポート	22/tcp
説明	リモートSSHサーバーは、SHA-1HMACアルゴリズムを有効にするように構成されています。 NISTはデジタル署名用のSHA-1の使用を正式に廃止していますが、HMACのセキュリティは衝突に強い基盤となるハッシュ関数に依存しないため、SHA-1は依然としてHMACに対して安全であると考えられています。 注意：このプラグインは、リモートSSHサーバーのオプションのみをチェックします。
対策	該当なし
出力	The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1 The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported : hmac-sha1
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.4

危険度	情報
検査項目	サポートされているSSHのアルゴリズムおよび言語
対象ポート	22/tcp
説明	このスクリプトは、通信を暗号化するためのリモートサービスによってサポートされているアルゴリズムおよび言語を、検出します。
対策	該当なし
出力	Scanner negotiated the following encryption algorithm with the server : The server supports the following options for kex_algorithms : curve25519-sha256 curve25519-sha256@libssh.org diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 kexguess2@matt.ucc.asn.au The server supports the following options for server_host_key_algorithms : rsa-sha2-256 ssh-rsa The server supports the following options for encryption_algorithms_client_to_server : aes128-cbc aes128-ctr aes256-cbc aes256-ctr The server supports the following options for encryption_algorithms_server_to_client : aes128-cbc aes128-ctr aes256-cbc aes256-ctr The server supports the following options for mac_algorithms_client_to_server : hmac-sha1 hmac-sha2-256 hmac-sha2-512 The server supports the following options for mac_algorithms_server_to_client : hmac-sha1 hmac-sha2-256 hmac-sha2-512 The server supports the following options for compression_algorithms_client_to_server : none The server supports the following options for compression_algorithms_server_to_client : none
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.5

危険度	情報
検査項目	SSHサーバーのタイプとバージョン情報
対象ポート	22/tcp
説明	空の認証要求を送信することにより、リモートSSHサーバーに関する情報を取得することができます。
対策	該当なし
出力	SSH version : SSH-2.0-dropbear SSH supported authentication : publickey,password
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.6

危険度	情報
検査項目	サービス検出
対象ポート	22/tcp
説明	本セキュリティ診断は、バナーによって、またはHTTPリクエストを受信したときに送信するエラーメッセージを確認することで、リモートサービスを識別できました。
対策	該当なし
出力	An SSH server is running on this port.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.7

危険度	情報
検査項目	SYNスキャナー
対象ポート	22/tcp
説明	このプラグインは、SYN「ハーフオープン」ポートスキャナーです。ファイアウォールで保護されたターゲットに対しても、適度な速さを維持する必要があります。 SYNスキャンは、破損したサービスに対するTCP（フル接続）スキャンより煩わしくありませんが、ネットワークに負荷がかかっている場合に、ファイアウォールの堅牢性を低下させるという問題を引き起こしたり、リモートターゲットで接続をオープンのまま残したりする可能性があります。
対策	IPフィルターでターゲットを保護します。
出力	Port 22/tcp was found to be open
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

5.付録

5.1 危険度判定基準

静的な重大度と動的な脆弱性優先度評価（VPR）を使用して、脆弱性をどれだけ緊急に修正する必要があるかを定量化します。静的な重大度の指標として、一般的にCVSSが使用されることが多いのですが、CVSSでは、高～重大に判定される脆弱性が比較的多いため、優先度を決めて対応することが困難だとの見解が一般的です。

本報告書では、以下のような脅威インテリジェンス情報を反映させた指標であるVPRを使用しています。技術的な脅威に加えて、攻撃のトレンドや攻撃の難易度を把握することで、より的確な危険度の判定が可能となります。

脅威インテリジェンスのイベント

- 脆弱性の悪用
- 公開リポジトリへの脆弱性エクスプロイトコードの投稿
- 主流メディアの脆弱性に関する議論
- 脆弱性に関するセキュリティ調査
- ソーシャルメディアチャネルの脆弱性に関する議論
- ダークウェブとアンダーグラウンドの脆弱性に関する議論
- ハッカーフォーラムの脆弱性に関する議論

VPRスコア範囲による分類基準

危険度	VPRスコアの範囲
重大	9.0～10.0
高	7.0～8.9
中	4.0～6.9
低	0.1～3.9
情報	0または値なし

5.2 評価基準

本報告書における総合評価は、以下に規定される絶対評価によるものです。絶対評価は、A、B、C、D のいずれかのアルファベット1文字で表記され、検査結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

評価レベル	評価基準	検出件数
A	早急に対策が必要な脆弱性は検出されませんでした。	検出件数0件
B	直接的に被害を受ける可能性は低いと推測されますが、脆弱性が確認されております。検出内容を確認の上、対策の検討を行うことを推奨します。	危険度高以上の脆弱性は1件も検出されていないが、危険度中以下の脆弱性検出件数は1件以上
C	被害を受ける可能性のある脆弱性が確認されております。早急に対策の検討を行うことを推奨します。	危険度重大以上の脆弱性は1件も検出されず、危険度高の脆弱性が1件以上検出
D	大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。	危険度重大の脆弱性が1件以上検出

5.3 免責事項

危険度判定基準は、あくまでも目安であり、脆弱性の検出された箇所・内容等により判定基準とは異なる危険度を脆弱性に与えることもございますので、あらかじめご了承ください。

評価基準は本検査において検出された脆弱性の検出件数を基に、検査結果を簡潔に表現するために作成された独自基準になります。上記評価基準による評価は、あくまでも検査結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますので、あらかじめご了承ください。

本報告書の対策を実施する前に、対策の影響度について検討し、対応の可否をご判断ください。弊社では、設定変更後のトラブルについて、責任を負いかねます。また、本報告書の対策によって、全てのセキュリティ対策を網羅できるものではない事についてご了承下さい。

具体的な対策方法については販売代理店様、メーカー様に別途お問合せください。

また、弊社は検査結果により生成された情報及び本報告書に記載された事項に関して、是正処置等の責任を負わないものとします。

その他、以下URLから参照可能なサービス利用規約に準じます。

https://www.singleid.jp/wp-content/uploads/2021/09/SingleID_UserAgreement.pdf

5.4 お問い合わせ

本報告書に関するご質問は、報告書のご提出日より起算して１か月承ります。

また、本レポートを基に対策を実施される場合に、個別の実施方法についてのご質問にはお答えしかねますことをご了承下さい。

お問合せ先　https://www.singleid.jp/contact/