CONFIDENTIAL

SAMPLE

○○○○○株式会社　御中

プラットフォーム診断
診断結果報告書
【速報】

脆弱性診断後 3 営業日以内に提出いたします。
本診断結報告書では危険度の高い脆弱性(Medium 以上)の技術的な対処方法・対策方法の説明を報告いたします。

平成○○年○月○日

株式会社 ソフテック

CONFIDENTIAL

SAMPLE

【資料改編履歴】

日 付	内 容	承 認	作成/更新
平成○○年○月○日	第一版作成	○○	○○

CONFIDENTIAL

SAMPLE

目　　次

1　目的

本診断結果報告書【速報】は、平成〇〇年〇月〇日に実施したプラットフォーム診断において、深刻な影響を与えることが懸念される脆弱性をより早くご報告するために、診断結果の一部を抽出、要約したものです。

深刻な影響を与えることが想定される脆弱性をより早くご報告することで、正式な診断報告を待つことなく、脆弱性への対応を行うことが可能です。

なお、本診断結果報告書【速報】はあくまでも現時点での調査結果・要約という位置付けの報告であり、最終的な診断結果報告書とは内容が異なる場合もございますので、ご了承下さい。

2　診断対象

本診断における診断対象は以下の通りです。

No	IP アドレス	サーバ名	備考
1	192.168.1.1	公開用 Web サーバ	
2			
3			
4			

3　診断結果要約

本診断において、現時点で危険性が高いと考えられる脆弱性は確認されておりません。サーバソフトウェアの設定等に起因した、軽微な脆弱性のみを確認しております。

検出された軽微な脆弱性については、「４　その他の脆弱性一覧」をご参照下さい。

4　その他の脆弱性一覧

現時点で本診断において検出されている脆弱性の内、「3　診断結果要約」にて示した危険性の高い脆弱性以外のものについて表 4-1 に示します。

なお、これらの脆弱性については全て危険度 Low となります。各脆弱性の詳細・対策につきましては診断結果報告書に記載させて頂きます。

表 4-1　その他の脆弱性一覧

脆弱性名称（診断項目）	脆弱性内容
推測可能な SNMP コミュニティ名の使用（設定不備によるシステム情報漏洩）	対象サーバ [対象ポート] 192.168.1.1 [161/udp] 概要 対象サーバにおいて、推測可能なコミュニティ名による SNMP プロトコルでの情報取得が可能であることを確認しております。 SNMP（Simple Network Management Protocol）とは、ネットワークに接続された通信機器（ルータやコンピュータ等）をネットワーク経由で監視・制御するためのプロトコルです。 SNMP におけるコミュニティ名は、監視・制御の対象機器と通信する際に使用されるものでパスワードと同じように重要な意味を持つものです。 SNMP 製品の多くはデフォルト値として public を使用していることから、コミュニティ名をデフォルト値のまま使用している場合、ネットワーク機器に関するシステム情報等が漏洩する可能性があります。 snmpwalk コマンドによる出力結果より、Linux のカーネルバージョンを始めとしたシステム情報が容易に取得可能な状態であることから、SNMP のコミュニティ名について推測困難な文字列に変更するか、UDP ポート番号 161 へのアクセス制限を行うことを推奨します。

5　危険度の判定基準

本診断結果報告書【速報】では検出された各脆弱性について、表 5-1 を基に危険度を判定し記載しています。

危険度は、検出された各脆弱性への対策の際に、どの脆弱性を優先的に修正すべきか判断するための目安として記載しているものです。

表 5-1　危険度の判定基準

危険度	判定基準
Critical	ネットワーク経由で管理権限を奪取される等、深刻な被害を受けることが懸念される脆弱性。
High	潜在的に重大な被害を受ける可能性のある脆弱性。
Medium	単体では被害を受ける可能性は低いが、他の脆弱性と組み合わせることで被害を受けることが想定される脆弱性。
Low	Medium 以上には該当しない、現時点では被害を受ける可能性が低いと考えられる脆弱性。

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ありますので、ご了承下さい。

6　実施した診断項目一覧

本診断において行った診断項目一覧を以下に示します。

不正侵入

不正侵入が想定される脆弱性に関わる診断を行いました。

項目名	内容
不正なログイン	ログイン権限を持たない、もしくは、正規のユーザでないユーザが不正にログイン出来ることが想定される脆弱性に関わる診断を行いました。デフォルトアカウント（アプリケーションインストール時等に自動的に登録されるアカウント）の放置や、脆弱なパスワードを持つアカウント等、不適切なユーザ管理についての診断を含みます。
ネットワーク上からのプログラム実行	ネットワーク上から不正なプログラムを実行可能なことが想定される脆弱性に関わる診断を行いました。
特権ユーザ権限の奪取	一般ユーザから正規の手順以外の方法で管理者権限やその他特別な権限を取得することが想定される脆弱性に関わる診断を行いました。
バックドアプログラムの存在	バックドア（裏口）プログラムが動作していないか診断を行いました。

サービス妨害

動作しているサービスを妨害や停止させることが想定される脆弱性に関わる診断を行いました。

項目名	内容
サービス妨害・停止	サービスを妨害もしくは停止される可能性のある脆弱性について診断を行いました。なお、本項目での診断では実際に攻撃は行わず、主にサーバのバージョン情報等から脆弱性を推測して検出しました。
DDoS エージェントの存在	DDoS（分散型サービス妨害攻撃）に使用されるエージェントプログラムが動作していないか診断を行いました。

情報漏洩

システム情報、ユーザ情報等の漏洩が想定される脆弱性に関わる診断を行いました。

項目名	内容
ネットワーク上からのファイル取得	ネットワーク上からファイルが取得可能な脆弱性について診断を行いました。主に NFS（Network File System）や FTP（File Transfer Protocol）、Windows のファイル共有等、リモートホスト間でファイルを送受信することが可能なサービスの設定不備によるファイル取得について検出を行いました。
不要なサービスの動作	ポートスキャンを行い、一般的に動作させておく必要が無いと思われるサービスが動作していないか診断を行いました。
サーバプログラムのバージョン取得	ヘッダ情報等によるサービスプログラムのバージョンの取得について診断を行いました。
設定不備によるシステム情報漏洩	OS やサーバプログラムの設定不備によるシステム・ユーザ情報漏洩の存在について診断を行いました。
既知の脆弱性による情報漏洩	FTP サーバや Web サーバ等、サーバ事態に存在する既知の脆弱性による情報漏洩について診断を行いました。

以上