CONFIDENTIAL

2022年4月1日

株式会社AGEST　御中

「株式会社AGEST」

プラットフォーム診断
結果報告書

目次

1. エグゼクティブサマリー

総合評価	危険	大規模な影響を及ぼす可能性のある脆弱性が検出されました。

本診断の総合評価と、その定義は次のとおりです。

評価	解説
緊急	攻撃への利用が容易で直接的な被害を及ぼす可能性のある脆弱性が検出されました。 緊急の対策が必要です。
危険	大規模な影響を及ぼす可能性のある脆弱性が検出されました。早急に対策が必要です。
警告	**間接的にまたは複数組み合わせることで攻撃に利用され、 実害を受ける可能性のある脆弱性を検出しました。計画的な対策が必要です。**
注意	被害を受ける可能性は低い、またはサービス提供に影響は小さいものの、 対策が推奨される脆弱性を検出しました。
問題なし	脆弱性は検出されませんでした。現在の対策を継続してください。

1.1 総評

本診断において、深刻度の高い問題としてすでにサポートが切れているPHPの使用を検出しております。
PHP 7.3系は2021年12月6日で開発元からのセキュリティサポートが終了しております。サポート終了後に報告された脆弱性に対して無防備となりますので、今後も使用を続けることは重大なセキュリティリスクとなります。早急にサポートバージョンへ切り替えてください。

その他、深刻度中程度の問題として、TLS1.0 , 1.1の使用を検出しております。暗号に関しては、CRYPTREC , IPAが暗号強度の調査を行っており、TLS1.0 , 1.1はそれらから安全でないとみなされております。これらの暗号を使用した場合、通信内容を復号され、機密情報を取得される恐れがあります。

ソフトウェアの脆弱性については各ベンダーが公開しているセキュリティアップデート情報から、暗号についてはCRYPTREC , IPAが公開しているガイドライン等から情報を得ることができます。
今後も新たな脆弱性が報告されていくことが予想されますので、被害を未然に防ぐために、こうした情報を収集しできる限り早く対応を行うようにしてください。

1.2 検出事項一覧

本診断にて検出された脆弱性は次のとおりです。個別の解説については 4. 以降から参照ください。

深刻度（検出数）	検出事項
Critical(0)	-
High(1)	• サポート切れソフトウェアの使用
Medium(1)	• 安全でない暗号化通信プロトコルの使用
Low(1)	• 非NLAでの接続が可能
Info(1)	• SSHサービスの公開

2. 診断の概要

2.1 診断目的

プラットフォーム診断（以後、「本診断」という）は、2.3 に係る様々な情報セキュリティ上の脆弱性の存在についての調査と、その結果の分析及び報告を行うものです。

2.2 診断日

本診断の診断実施日は次のとおりです。

> 実施日： 2022 年 4 月 1 日～2022 年 4 月 1 日

2.3 診断対象

本診断の対象となったサーバは次のとおりです。

- agest.co.jp
  - ■■■■■■
- www.agest.co.jp
  - ■■■■■■

※サンプルのため■■■と記載されている箇所がありますが、
実際の報告書ではマスク処理を行いません。

2.4 診断実施形態

本診断の診断実施形態は次のとおりです。

> 診断形態： リモート診断
> 診断場所： 株式会社AGEST 診断作業エリア

2.5 診断方法

本診断では、診断技術者による手動オペレーションを主とし、診断ツールを併用した診断を実施しました。

2.6 脆弱性診断観点

本診断では、以下の観点による脆弱性診断を行い、
攻撃が可能な脆弱性を実際に攻撃し、入手できる情報や被害を診断しました。

No	診断項目	解説	危険度
1	ネットワークの設定不備	各種ネットワークコマンドを実行し、その応答による各ホストの稼動状態の確認、ネットワークの経路情報収集、およびネットワーク規模に関する情報収集などを行います。 ネットワークコマンドの応答を基に、フィルタリング設定の不備等による情報漏洩の可能性がないかを診断します。	low
2	脆弱なサービスの存在	各ホストでどの様なサービス（Web サービスやメールサービス等）が稼働しているか情報収集を行います。 具体的にはサービスを提供する窓口となるポートの稼動状態をポートスキャンにより確認します。 さらに、稼動しているポートからバナーと呼ばれる情報を収集することで、サービスのソフトウェア名を特定します。 稼動しているポート番号および、ソフトウェア名を基に、運用上不要と考えられるサービスが稼働していないか、また、バックドアなどの不正プログラムが稼働していないかを診断します。	High～low
3	脆弱な古いバージョンのOS・サービス	各ホストで稼働しているポートからバナーと呼ばれる情報を収集することで、OS 種別やサービスのソフトウェア名、バージョンを特定します。 また、サービスに対して特定の診断データを与えた際の挙動により、バージョンを特定します。 このバージョン情報を基に、脆弱な古いバージョンが使用されていないかを診断します。	High
4	OS・ミドルウェアの設定不備	各ホストで稼働しているサービスの挙動を確認することで、OS・ミドルウェアの設定状況を確認します。確認された設定の不備を利用して、侵入や情報収集が行えるかを診断します。	High～low

No	診断項目	解説	危険度
5	不要なコンテンツやスクリプト	Webサービスやミドルウェアなどのインストール時、デフォルトでインストールされるコンテンツおよびサンプルスクリプトの有無を確認します。 確認されたサンプルスクリプトを利用して、侵入や情報収集が行えるかを診断します。	Medium ～low
6	暗号化通信の不備	各ホストで稼働しているサービス情報から、暗号化されていない管理系サービス(Telnet や FTP など)が使用されていないかを診断します。 また、暗号化通信が使用されている場合、脆弱なバージョンのプロトコルや暗号化スイートの指定が許可されていないかを診断します。	Medium
7	推測可能なパスワード	パスワード認証を伴うサービスに対して、システムに登録されているユーザIDとパスワードを推測してシステム（またはサービス）への侵入を試みます。 攻撃者がよく用いるパスワード（デフォルトパスワード、管理者が登録しがちなパスワード）を利用して、脆弱なパスワードが設定されているかどうかのチェックを行います。	High
8	第三者によるメールの不正中継	メールサービスに対して、通常の送信者名(From)と受信者(To)のパターンの他に100パターン以上の組合せでメールの不正中継を試みます。 不正中継のパターンチェックが厳密でない場合、メールサーバがSPAMの踏み台にされる可能性があります。	High

2.7 危険度について

本診断では、発見された問題について「危険度」という尺度で対応の優先度を表しています。
この危険度の判定は主にCVSS を参考として「Critical」「High」「Medium」「low」の4段階に分類されます。

危険度	CVSS	解説
Critical	9.0-10.0	危険度高の攻撃の中でも特に対応が急がれるものです。
High	6.0-8.9	攻撃者による侵入行為やサービス使用不能攻撃、重要情報漏洩に直接結びつく脆弱性です。 確認された脆弱性によって貴社の機密情報が改ざん・破壊・漏洩等の被害を受けた場合、社会的信用問題に発展する可能性があります。
Medium	3.0-5.9	複数の条件が揃った場合、侵入行為やサービス使用不能攻撃に結びつく脆弱性です。 確認された脆弱性を組み合せることによって攻撃が成立する可能性があります。
low	0.1-3.0	現時点で攻撃に結びつきませんが、侵入を試みている攻撃者に対し攻撃の手掛かりとなる情報を与える脆弱性です。 対策を施す事により、攻撃者に対しセキュリティレベルの高いホストであるという印象を与える事ができます。

2.8 特記事項

特になし

3. 診断結果詳細

【オープンポート情報の記載内容について】
TCP/UDP ともに Well Known ポート(1～1023 番)および High ポート（1024～65535 番）についてスキャンを実施しました。 UDPに関してはプロトコルの性質上、正しい結果が得られない可能性があります。
また、ルータ及びファイアウォールでフィルタリングされている場合には、実際のオープンポート情報と異なる結果が出力される場合があります。

3.1 診断対象別 OS推測/FQDN/CPE列挙

ドメイン名/IPアドレス	OS推測	FQDN	CPE
agest.co.jp	Linux Kernel 2.6	■■■■■■	cpe:/o:linux:linux_kernel cpe:/a:■■■■:■■■■■■
www.agest.co.jp	Microsoft IIS	■■■■■■	cpe:/a:microsoft:iis cpe:/a:■■■■:■■■■■■

3.2 オープンポート情報

- オープンポート情報(TCP)

ドメイン名/IPアドレス	ポート	サービス名	バージョン情報
agest.co.jp	22	ssh	■■■■■■
	80	http	■■■■■■
	443	https	■■■■■■
	■■■	■■■	■■■■■■
www.agest.co.jp	80	http	■■■■■■
	443	https	■■■■■■
	3389	ms-wbt-server	■■■■■■

- オープンポート情報(UDP)
  取得できず
- ユーザ情報
  取得できず

4. 個別検出事項

4.1 Critical

該当なし

4.2 High

4.2.1 サポート切れソフトウェアの使用

深刻度：High

問題とその原因

診断対象において、サポートが終了しているソフトウェアの使用が検出されました。 PHP 7.3系は2021年12月6日で開発元からのセキュリティサポートが終了しております。※

- 検出したソフトウェア：PHP/7.3.0

```
curl -ik https://agest.co.jp/cgi-bin/index.php

HTTP/1.1 200 OK
Content-Type: text/html;charset=utf-8
Server:
X-Powered-By: PHP/7.3.0
(以下略)
```

※
検出されたバージョン情報からサポート期限を調査し報告しております。

想定される被害

サポート終了しているソフトウェアは新しいセキュリティパッチがベンダーからリリースされないため、サポート終了より後に発見された脆弱性に対して無防備となります。

CVSS

- CVSSによる評価なし

推奨する対策

- 最新版またはセキュリティ対策が施されているサポートバージョンに切り替えてください。

参考情報

「Supported Versions」(PHP)

- https://www.php.net/supported-versions.php

該当箇所

No.	ドメイン名	ポート番号
1	agest.co.jp	80,443

4.3 Medium

4.3.1 安全でない暗号化通信プロトコルの使用

深刻度：Medium

問題とその原因

診断対象において、プロトコルの仕様上に脆弱性のあるTLS1.0 , 1.1を有効化していることを検出しました。
TLS1.0 , 1.1は、IPA発行の「TLS暗号設定ガイドライン」で「セキュリティ例外型」に該当し "安全性上のリスクを受容してでも継続利用せざるを得ないと判断される場合にのみ採用すべきである"とされています。

```
nmap --script ssl-enum-ciphers -p 443 agest.co.jp
(中略)
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
(中略)
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
(以下略)
```

想定される被害

TLS1.0 , 1.1には、強度の弱い暗号アルゴリズムを強制的に使わせる "ダウングレード攻撃" の脆弱性が存在します。それに加えてTLS1.0では、CBCモードに対する"選択平文攻撃"を受ける脆弱性が存在します。
これらの攻撃によって、攻撃者に平文のデータを取得される恐れがあります。

CVSS

- Base Score：4.3

脆弱性対策情報データベース

- https://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-002305.html

推奨する対策

- TLS1.0 , 1.1を無効化し、TLS1.2以上のみが有効となるよう設定してください。

一般的な設定例となりますのでご確認ください。

【Apache】

ssl.confを下記の内容に変更してください。

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

【AWS ELBもしくはCloudfront】

AWS Webコンソールにて設定画面を開き、SecurityPolicyを下記のいずれかに変更してください。

```
AWS ELB (リスナーのセキュリティポリシー)
・ELBSecurityPolicy-FS-1-2-Res-2020-10
・ELBSecurityPolicy-FS-1-2-Res-2019-08
・ELBSecurityPolicy-FS-1-2-2019-08
・ELBSecurityPolicy-TLS-1-2-Ext-2018-06

AWS Cloudfront (Cloudfrontとビューワーとの間で使用する暗号)
・TLSv1.2_2021
・TLSv1.2_2019
・TLSv1.2_2018
```

参考情報

「TLS暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～」(ページ番号35)

- https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

「Deprecating TLS 1.0 and TLS 1.1」

- https://datatracker.ietf.org/doc/html/rfc8996

該当箇所

No.	ドメイン名	ポート番号	TLS1.0	TLS1.1
1	agest.co.jp	443	✓	✓
2	www.agest.co.jp	443	-	✓

4.4 Low

4.4.1 非NLAでの接続が可能

深刻度：Low

問題とその原因

診断対象において、リモートデスクトップ接続のNLA(ネットワークレベル認証)が必須となっていないことを検出しました。
リモートデスクトップ接続では、NLAによってサーバとのセッションを確立する前に認証が行えるため、攻撃者からの悪意あるパケットを受け取るリスクを減らすことができます。
また、Windowsのログイン画面では有効なユーザ情報を取得することが可能です。

検証では「enablecredsspsupport:i:0」を書き加えたRDPファイルを作成し(下記のdhtest.rdp)、非NLAでのリモートデスクトップ接続を行っております。

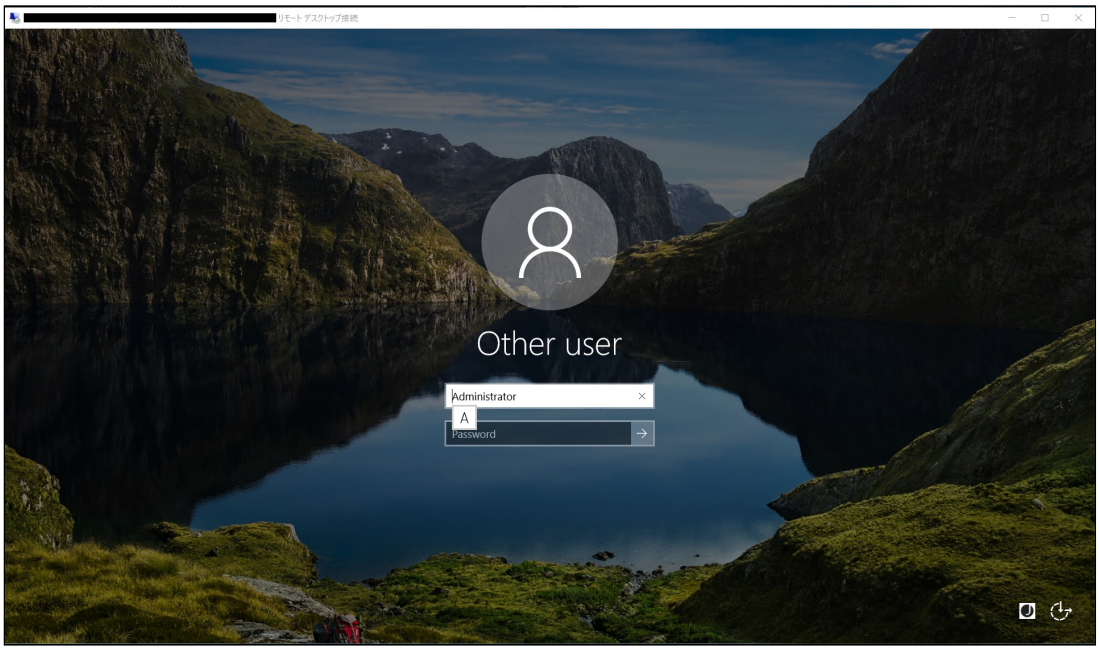

図1 ログイン画面

RDPファイルの内容：dhtest.rdp

```
full address:s:www.agest.co.jp
authentication level:i:2
enablecredsspsupport:i:0
```

想定される被害

ユーザ認証完了まで完全なリモートデスクトップ接続が行われないことで、攻撃者からの悪意あるパケットを受けるリスクを軽減できます。
また、有効なユーザ名がわかることで、未登録のユーザでパスワードを試すような無駄な作業をせずに効率よくパスワードクラッキングを行うことが可能なことから、不正アクセスの危険性が高まります。

CVSS

- CVSSによる評価なし

推奨する対策

- サーバのリモートデスクトップに関する設定にて「ネットワークレベル認証でリモートデスクトップを実行しているコンピューターからのみ接続を許可する」を有効としてください。

参考情報

「ネットワーク レベル認証でのみ接続を許可する理由」

- https://docs.microsoft.com/ja-jp/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access#why-allow-connections-only-with-network-level-authentication

---

該当箇所

No.	ドメイン名	ポート番号
1	www.agest.co.jp	3389

4.5 Info

4.5.1 SSHサービスの公開

深刻度：Info

問題とその原因

診断対象において、SSHサービスへ接続可能であることを確認しました。
SSHは利用者が組織内の人間に限られ、外部に公開する必要のないサービスであるため、 ポートフィルタリングなどによって、サービスの稼働を外部から判別できないようにすることを推奨いたします。

```
telnet agest.co.jp 22
Trying
Connected to agest.co.jp.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.0
(以下略)
```

想定される被害

接続時に表示される情報からソフトウェアのバージョン情報を取得されたり、辞書攻撃・ブルートフォース攻撃を受けアカウント情報を取得される恐れがあります。

CVSS

- CVSSによる評価なし

推奨する対策

- ポートフィルタリングなどによって、SSHサービスを非公開とすることを推奨いたします。

該当箇所

No	ドメイン名	ポート番号
1	agest.co.jp	22

5. 報告書の取り扱いについて

本報告書の取り扱いについては、以下の点にご注意ください。

- 本報告書には、本システムの情報セキュリティ事象についての重要な記述が含まれていますので、取り扱いには十分注意してください。
- 本報告書に記された診断結果や評価は、診断が実施された2022年4月1日時点のものであり、将来にわたり内容を保証するものではありません。
- 本報告書の著作権は弊社が所有しており、複製や改変、第三者への開示は原則禁止とします。ただし、システム管理者や経営者への報告、あるいは情報セキュリティ状況改善のため、資料として使用する等の場合においては、貴社と弊社との間に交わされた機密保持契約の定めるところに従い、配布することを許可します。