〇〇株式会社 御中

「サンプル・システム」
プラットフォーム脆弱性診断報告書

EG セキュアソリューションズ株式会社

2020 年〇月〇日

目次

1. エグゼクティブサマリー

1.1. 総合評価

中危険度(Medium)

1.2. 総評

脆弱性診断の結果、5 件の脆弱性および 1 件の改善指摘が発見されました。

発見された脆弱性として、SSL/TLS の設定に関する問題が複数あります。SSL/TLS が正しく使われていないため、通信路上に攻撃者が存在する場合、盗聴などの攻撃を受けやすくなります。

サーバー証明書のコモンネームの不一致が発見されています。中間者攻撃を受けやすくなるため、ホスト名と一致する正規のサーバー証明書の導入をお勧めします。

SSH の設定に関する問題があります。SSH が正しく設定されていないため、通信路上に攻撃者が存在する場合、盗聴などの攻撃を受けやすくなります。

FTP、SMTP、POP3 等の暗号化されないプロトコルが使われています。SSH、SMTP over SSL、POP3 over SSL 等の暗号化プロトコルの使用をお勧めします。

POODLE 脆弱性があります。利用者に中間者攻撃をしかけることにより、HTTPS 暗号化された情報の一部を第三者が解読できる可能性があります。

指摘事項として、TLS の上位バージョン(TLSv1.1, TLSv1,2)に対応していないことが挙げられます。TLS のバージョンが高いほど、暗号解読などの攻撃に対して堅牢になっています。TLS の上位バージョンに対応することによる副作用はないため、対応を推奨します。

1.3. 内在するリスク

1.3.1. 情報漏洩

指摘事項	危険性
2.2. SSL/TLS 設定の不備	**Medium**
2.3. サーバー証明書のコモンネームの不一致	**Medium**
2.4. CBC ブロック暗号をサポートする SSH の検出	**Medium**
2.5. 平文による認証が可能	**Low**
2.6. POODLE 脆弱性	**Low**
2.7. 新しい TLS バージョンに不対応	**Information**

1.4. 危険度の評価基準

危険度	説明
Critical	High レベルの危険度を保持し、かつ具体的な攻撃手順が発見された脆弱性です。
High	情報漏洩やシステムの停止を招く可能性のある脆弱性です。
Medium	複数の組み合わせにより実害に至る可能性のある脆弱性です。
Low	被害を拡大させる潜在的な脆弱性です。
Information	脆弱性ではありませんが、セキュリティ上および開発上の改善点です。

1.5. 対策指針

1.5.1. 早急の対策

発見された脆弱性は、サーバー設定の不備に起因しています。このため、該当箇所において適切なサーバー設定を行うことで、一般的なセキュリティ水準に引き上げが可能と考えられます。

1.5.2. 恒久的な対策

今回指摘されたような脆弱性がなぜ混入したか、その根本原因を分析する必要があります。多くの場合、サーバーエンジニアの知識不足や、ガイドライン類の未整備、開発後のテストの不足などが原因となっています。

原因は 1 つとは限らないため、複合的に予防処置をとり、継続的に開発プロセスの改善と開発メンバーの強化を進めることを推奨します。

2. 詳細

2.1. 診断サマリ

■診断対象		
No.	診断対象 IP Address	ホスト名
1	203.0.113.5	example.jp

■稼動状況		
ホスト名	IP アドレス	判定 OS
example.jp	203.0.113.5	不明だが、Linux 2.6.18(CentOS5 等)と推定

■稼動アプリケーション

No.	サービス	アプリケーション	バナー	ポート
1	FTP	不明	220 203.0.113.5 FTP server ready.	21
2	SSH	OpenSSH	OpenSSH 5.3	22
3	SMTP	不明	220 XXXXX ESMTP	25
4	HTTP	Apache	Server:Apache	80
5	POP3	不明	+OK <XXXXX@XXXXX>	110
6	HTTPS	Apache	Server:Apache	443
7	HTTPS		SSLv3	443
8	HTTPS		TLSv1	443
9	SMTP	不明	220 XXXXX ESMTP	443
10	IMAP4	Dovecot	OK Dovecot ready.	587
11	POP3	Dovecot	+OK Dovecot ready.	993
12	HTTPS	Apache	Server:Apache	995

■検出された脆弱性

No.	脆弱性名	概要	危険度
1	SSL/TLS 設定の不備	SSL/TLS 設定の不備により盗聴等の危険性があります	Medium
2	サーバー証明書のコモンネームの不一致	サーバー証明書のコモンネーム不一致により、中間者攻撃を受けやすくなっています	Medium
3	CBC ブロック暗号をサポートする SSH の検出	SSH 設定の不備により盗聴等の危険性があります	Medium

4	平文による認証が可能	FTP、SMTP、POP3 にて平文の認証が有効になっています	Low
5	POODLE 脆弱性	SSLv3 に対応しているため POODLE 脆弱性による盗聴のリクスがあります	Low
6	新しい TLS バージョンに不対応	TLSv1.1、TLSv1.2 に対応していません。	Information

2.2. SSL/TLS 設定の不備

概要	
危険度	Medium
攻撃難易度	困難

説明

以下のポートは SSL/TLS が有効ですが、設定の不備および脆弱性が認められます。

110/TCP　POP3
587/TCP　SMTP

具体的には以下が認められます。

- SSLv2 および SSLv3 が有効
- SSLv3 プロトコルに POODLE 脆弱性
- 危殆化された暗号スイート RC4 が有効
- 自己署名証明書の使用
- 証明書の有効期限切れ
- Logjam 脆弱性

影響

通信路上に攻撃者が存在する場合、ネットワーク盗聴により認証情報（ID とパスワード）が漏洩する危険性や、秘密情報の漏洩の危険性があります。

対策

以下の両方の対策を推奨します。

- SSL をやめ、TLS による設定にする
- RC4 を含む暗号スイートを除外する
- 自己署名証明書をやめ、正規の証明書を導入する
- DH パラメータを 1024bit(可能であれば 2048bit)で独自に生成する（Logjam 対策）
- DH パラメータが明示的に指定できない場合は修正版にアップデートする（Logjam 対策）

該当サーバー

example.jp

2.3. サーバー証明書のコモンネームの不一致

概要	
危険度	Medium
攻撃難易度	困難

説明

以下のポートは SSL/TLS が有効ですが、サーバー証明書のコモンネームがホスト名と一致していません。

21/TCP FTP over SSL
25/TCP SMTP
143/TCP IMAP4
587/TCP SMTP
993/TCP IMAP4
995/TCP POP3

上記において、サーバー証明書のコモンネームは下記の通りであり、実際のホスト名と異なっています。

- example1.jp

影響

証明書の確認が適切に行われないため、通信路上に攻撃者が存在する場合、中間者攻撃を受けやすくなります。

対策

以下の対策を推奨します。

- ホスト名と一致する正規のサーバー証明書を導入する

該当サーバー

example.jp

2.4. CBC ブロック暗号をサポートする SSH の検出

概要	
危険度	Medium
攻撃難易度	困難

説明

TCP/22 ポートで検出した SSH サーバーが、既知の脆弱性がある Cipher Block Chaining（CBC）モードのブロック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復元することができます。

検証例

次のコマンドを実行して、SSH にてサポートされているアルゴリズムを確認します。

```
nmap -vv --script ssh2-enum-algos -p 22 203.0.113.5
```

結果

```
PORT     STATE SERVICE REASON
22/tcp open    ssh       syn-ack
| ssh2-enum-algos:
|     kex_algorithms: (12)
|         curve25519-sha256
|         curve25519-sha256@libssh.org
|         ecdh-sha2-nistp256
|         ecdh-sha2-nistp384
|         ecdh-sha2-nistp521
|         diffie-hellman-group-exchange-sha256
|         diffie-hellman-group16-sha512
|         diffie-hellman-group18-sha512
|         diffie-hellman-group-exchange-sha1
|         diffie-hellman-group14-sha256
|         diffie-hellman-group14-sha1
|         diffie-hellman-group1-sha1
|     server_host_key_algorithms: (5)
|         ssh-rsa
|         rsa-sha2-512
|         rsa-sha2-256
|         ecdsa-sha2-nistp256
```

```
|         ssh-ed25519
|     encryption_algorithms: (12)
|         chacha20-poly1305@openssh.com
|         aes128-ctr
|         aes192-ctr
|         aes256-ctr
|         aes128-gcm@openssh.com
|         aes256-gcm@openssh.com
|         aes128-cbc
|         aes192-cbc
|         aes256-cbc
|         blowfish-cbc
|         cast128-cbc
|         3des-cbc
|     mac_algorithms: (10)
|         umac-64-etm@openssh.com
|         umac-128-etm@openssh.com
|         hmac-sha2-256-etm@openssh.com
|         hmac-sha2-512-etm@openssh.com
|         hmac-sha1-etm@openssh.com
|         umac-64@openssh.com
|         umac-128@openssh.com
|         hmac-sha2-256
|         hmac-sha2-512
|         hmac-sha1
|     compression_algorithms: (2)
|         none
|_        zlib@openssh.com
```

コマンド実行結果の赤枠内を参照すると、Cipher Block Chaining（CBC）モードで使用するアルゴリズムがサポートされているのを確認できます。

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- blowfish-cbc
- cast128-cbc

CBC モードのブロック暗号化には脆弱性が報告されています。
攻撃に成功すると、ひとつの暗号化ブロックから 32 ビットの平文を取り出すことが可能です。

参考：
CVE-2008-5161
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5161
https://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001963.html

影響

通信路上に攻撃者が存在する場合、ネットワーク盗聴により、SSL/TLS によって保護されている通信が、攻撃者に解読されるおそれがあります。

対策

CBC（Cipher Block Chaining）モードではなく CTR（CounTeR）モードを使用するために、SSH サーバー設定ファイル「/etc/ssh/sshd_config」に以下の文字列を追加します。

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

SSH サーバー設定ファイルに、既に「Ciphers」エントリが存在している場合は、「Ciphers」行に列挙されている値のうち、「-cbc」を含む文字列を削除してください。

設定変更後は SSH サーバーを再起動して、ご使用中の SSH クライアントから正常に通信できることを確認してください。

該当サーバー
example.jp

2.5. 平文による認証が可能

概要	
危険度	**Low**
攻撃難易度	困難（ネットワーク経路上に攻撃者が存在する場合は容易）

説明

以下のポートは平文による認証となるため、認証情報が外部に漏洩する危険性があります。

21/TCP　FTP
25/TCP　SMTP
587/TCP　SMTP
8000/TCP HTTP

影響

通信路上に攻撃者が存在する場合、ネットワーク盗聴により認証情報（ID とパスワード）が漏洩する危険性や、秘密情報の漏洩の危険性があります。

対策

SSH、SMTP over SSL、HTTPS 等の暗号化プロトコルの使用をお勧めします。FTP に関しては FTPS(FTP over SSL)、SMTP に関しては SSL/TLS のポートが用意されているので、実質的に問題となるのは 8000 番の HTTP のみです。

該当サーバー

example.jp

2.6. POODLE 脆弱性

概要	
危険度	**Low**
攻撃難易度	困難

説明

SSLv3 に対応しているため、POODLE 脆弱性により情報（典型的には Cookie）が窃取され、情報漏洩につながる可能性があります。

具体的には、通信路上にいる攻撃者が利用者の通信を横取りして中間者攻撃(MITM)を仕掛けることにより、情報の一部を解読できることが指摘されています。

影響

罠サイトを閲覧した利用者に対して、SSL 通信の一部を盗聴される可能性があります。

該当サーバー

example.jp

2.7. 新しい TLS バージョンに不対応

概要	
危険度	**Information**
攻撃難易度	困難

説明

TLSv1.1、TLSv1.2 に対応していません。新しいバージョンの TLS ほど盗聴などの攻撃に対して堅牢なので、これらを有効化することを推奨します。

影響

通常は問題となりませんが、非常に高度な攻撃を受けた場合に影響があります。たとえば、暗号鍵が漏洩した状況で、過去に盗聴された情報までさかのぼって暗号解読されるリスクが高まります。

対策

TLSv1.1、TLSv1.2 を有効化してください。

該当サーバー

example.jp

3. 診断概要

3.1. 診断情報

プラン	ネットワーク脆弱性診断
IP アドレス	203.0.113.5
ホスト名	example.jp
診断方法	Nessus によるツール診断、手動による確認作業
サービス状態	本番稼働前環境
アクセス方法	インターネット経由
診断実施者	徳丸　浩
診断期間	2020/〇/〇～2020/〇/〇
診断時間	9:00 ～ 18:00

4. 免責

4.1. 診断の正確性

ネットワーク脆弱性診断は、診断対象サーバーに対して、診断ツールを操作して行なうブラックボックス・テストを実施しております。

脆弱性診断の特性上、本報告書に記載する脆弱性については再現性・網羅性を完全に保証するものではありません。脆弱性への対策指針をもとにパッチ適用やサーバー設定その他の対策を行なわれる場合、貴社の責任で行なって頂きますようお願いします。

4.2. 本報告書に関するお問合せ

本報告書に関するご質問・その他お問い合わせは、本報告書のご提出日より起算して 1ヶ月間承ります。ただし、本報告書をもとにお客様がプログラム修正などの対策を実施される場合については、個別の実装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ください。

期間終了後のお問い合わせについては、別途ご相談ください。

お問合せ先： contact@eg-secure.co.jp