2018年09月18日発行
注文番号：00000000

セキュリティー診断レポート

株式会社ニジモ
東京都渋谷区渋谷1-12-2
クロスオフィス渋谷5F
TEL: 03-6712-6011
FAX: 03-6712-6012

はじめに

FujiSSL-Premiumセキュリティー診断結果につきましてご案内いたします。

レポートの結果に応じ、案内に関する情報は青、警告に値する情報は黄、危険に値する情報は赤の配色にてご説明しておりますので詳しくは各診断項目をご確認ください。

診断では実際に脆弱性を利用した攻撃を実施しているわけではありませんので、検知された脆弱性は誤検知である可能性があります。

概要説明

診断概要

診断日時：2018年09月18日 18時45分
診断対象FQDN：www.example.com

お客様情報

申請組織・団体名：株式会社ニジモ
お客様名：NIJIMO TARO
郵便番号：150-0002
都道府県：東京都
市区町村：渋谷区
住所：渋谷1-12-2
ビル・マンション名：クロスオフィス渋谷5F
電話番号：03-0000-0000
メールアドレス：yourname@example.com

診断結果

証明書プロパティ

■ Common Names

説明： Common Name(コモンネーム)とは、SSLサーバ証明書の設定項目の一つで、SSL暗号化通信を行うサイトのURLのうち、サブドメインまでを含んだドメイン部分の名称を示します。
結果： www.example.com

■ Alternative names

説明： SSLサーバ証明書の拡張領域「Subject Alternative Names（サブジェクトの別名）」（以下 SANs）に登録されたコモンネームがある場合、CSRに指定したコモンネーム（FQDN）とは別に、SANsに登録されたコモンネームへもSSL通信が 可能となります。
結果： DNS:www.example.com,DNS:example.com

■ Serial Number

説明： 認証局が発行した証明書に一意に付けられる番号です。
結果： 12:b9:b0:fa:72:e0:d8:48:c6

■ Valid from

説明： 証明書の有効開始日時になります。
結果： 2017-08-30 13:35:09

■ Valid until

説明： 証明書の有効期限になります。
結果： 2020-09-13 13:55:00

■ Issuer

説明： 証明書を発行した組織情報になります。
結果： FujiSSL Public Certification Authority - G1

■ Key

説明： 証明書暗号化アルゴリズムの形式になります。
結果： rsaEncryption (2048 bit)

■ Signature algorithm

説明： 署名アルゴリズムの形式になります。
結果： sha256WithRSAEncryption

■ Certificate Transparency

説明： 認証局が証明書を発行する都度、全ての証明書発行の証跡を、第三者の監査ログに記載する仕組みです。主に、ウェブサイトの運営者やドメイン名の管理者が、その監査ログサーバ（以下「ログ）を確認することで、自分のドメインに対して不正な証明書や、ポリシー外の認証局からの証明書が発行されていないかを検証することができます。それにより利用者が不正に発行された証明書を信頼することを防止する為の機能になります。
結果： disabled
警告： Certificate Transparencyが有効になっておりません。
対応： 証明書の再発行及び反映が証明書再発行手順
https://www.fujissl.jp/support/reissue/

■ Revocation informatio

説明： 失効リスト取得先情報になります。
結果：

Full Name:
URI:http://repo1.secomtrust.net/sppca/nijimo/fullcrl.crl

OCSP - URI:http://nijimo.ocsp.secomtrust.net

■ DNS CAA

説明： ドメインの管理者がDNSのCAA (Certification Authority Authorization)レコードを利用し、ドメイン名とサブドメインに対して証明書を発行できる認証局 (CA) を指定する機能です。
結果：
警告： CAAレコードが設定されておりません。このままでも問題ありませんが、証明書の発行を許可する認証局を指定する事で第三者が別の証明書を発行する事を防ぐ事ができます。
対応： CAAレコード設定例
https://www.fujissl.jp/info/1116/

通信プロトコル

■ Protocols

説明： ご利用されている通信プロトコル情報になります。

結果：

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

警告： 古いプロトコルでの通信が許可されており「POODLE脆弱性」の恐れがあります。SSLで保護されたウェブサイトとブラウザの間で、ハッカーの通信傍受や暗号解読の可能性があります。

危険： 通信プロトコルが古い為、「POODLE」及び「Heartbleed」の恐れがあります。SSLで保護されたウェブサイトとブラウザの間で、ハッカーの通信傍受や暗号解読の危険性があります。

対応： SSL通信設定にてTLS 1.2及び1.3以外は無効にしてください。
TLS 1.1以上のプロトコルに対応していない場合はSSL・TLSプロトコルのソフトウェアを最新版にアップデートしてから設定してください。

■ Cipher Suites

説明： 暗号スイート (Cipher Suites)
は、通信情報をを部分的に異なる暗号技術の組み合わせを定義するものです。

結果：

TLSv1
TLSv1 256 bits ECDHE-RSA-AES256-SHA
TLSv1 256 bits DHE-RSA-AES256-SHA
TLSv1 256 bits DHE-RSA-CAMELLIA256-SHA
TLSv1 256 bits AES256-SHA
TLSv1 256 bits CAMELLIA256-SHA
TLSv1 128 bits ECDHE-RSA-AES128-SHA
TLSv1 128 bits DHE-RSA-AES128-SHA
TLSv1 128 bits DHE-RSA-SEED-SHA
TLSv1 128 bits DHE-RSA-CAMELLIA128-SHA
TLSv1 128 bits AES128-SHA
TLSv1 128 bits SEED-SHA
TLSv1 128 bits CAMELLIA128-SHA
TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA
TLSv1 112 bits EDH-RSA-DES-CBC3-SHA
TLSv1 112 bits DES-CBC3-SHA
TLSv1 112 bits IDEA-CBC-SHA
TLS11
TLS11 256 bits ECDHE-RSA-AES256-SHA
TLS11 256 bits DHE-RSA-AES256-SHA
TLS11 256 bits DHE-RSA-CAMELLIA256-SHA
TLS11 256 bits AES256-SHA
TLS11 256 bits CAMELLIA256-SHA
TLS11 128 bits ECDHE-RSA-AES128-SHA
TLS11 128 bits DHE-RSA-AES128-SHA
TLS11 128 bits DHE-RSA-SEED-SHA
TLS11 128 bits DHE-RSA-CAMELLIA128-SHA
TLS11 128 bits AES128-SHA
TLS11 128 bits SEED-SHA
TLS11 128 bits CAMELLIA128-SHA
TLS11 112 bits ECDHE-RSA-DES-CBC3-SHA
TLS11 112 bits EDH-RSA-DES-CBC3-SHA
TLS11 112 bits DES-CBC3-SHA
TLS11 112 bits IDEA-CBC-SHA
TLS12
TLS12 256 bits ECDHE-RSA-AES256-GCM-SHA384
TLS12 256 bits ECDHE-RSA-AES256-SHA384

TLS12 256 bits ECDHE-RSA-AES256-SHA
TLS12 256 bits DHE-RSA-AES256-GCM-SHA384
TLS12 256 bits DHE-RSA-AES256-SHA256
TLS12 256 bits DHE-RSA-AES256-SHA
TLS12 256 bits DHE-RSA-CAMELLIA256-SHA
TLS12 256 bits AES256-GCM-SHA384
TLS12 256 bits AES256-SHA256
TLS12 256 bits AES256-SHA
TLS12 256 bits CAMELLIA256-SHA
TLS12 128 bits ECDHE-RSA-AES128-GCM-SHA256
TLS12 128 bits ECDHE-RSA-AES128-SHA256
TLS12 128 bits ECDHE-RSA-AES128-SHA
TLS12 128 bits DHE-RSA-AES128-GCM-SHA256
TLS12 128 bits DHE-RSA-AES128-SHA256
TLS12 128 bits DHE-RSA-AES128-SHA
TLS12 128 bits DHE-RSA-SEED-SHA
TLS12 128 bits DHE-RSA-CAMELLIA128-SHA
TLS12 128 bits AES128-GCM-SHA256
TLS12 128 bits AES128-SHA256
TLS12 128 bits AES128-SHA
TLS12 128 bits SEED-SHA
TLS12 128 bits CAMELLIA128-SHA
TLS12 112 bits ECDHE-RSA-DES-CBC3-SHA
TLS12 112 bits EDH-RSA-DES-CBC3-SHA
TLS12 112 bits DES-CBC3-SHA
TLS12 112 bits IDEA-CBC-SHA

POODLE診断

概要

POODLEとは「Padding Oracle On Downgraded Legacy Encryption」の頭文字を組み合わせたので、SSLのバージョン3.0に存在する脆弱性(CVE-2014-3566)を指します。

この脆弱性を突くことで、悪意のある攻撃者は、第三者の通信に介在してSSL/TLSを脆弱なバージョン(SSL3.0)に落とし、通信させることができます。

この結果、SSL 3.0や実装が不十分なTLS1.0/1.1を有効にしているサーバとの通信においてパスワード等の個人情報やCookie情報が第三者に漏えいする危険性があります。

診断結果

古いプロトコルでの通信が許可されており「POODLE脆弱性」の恐れがあります。SSLで保護されたウェブサイトとブラウザの間で、ハッカーの通信傍受や暗号解読の可能性があります。

通信プロトコルが古い為、「POODLE」の恐れがあります。SSLで保護されたウェブサイトとブラウザの間で、ハッカーの通信傍受や暗号解読の危険性があります。

解決方法

TLS1.2及び、TLS1.3以外のプロトコルは無効にしてください。

許可しているプロトコルを全て無効にして頂き、TLS1.2及び、TLS1.3のプロトコルを有効にしてください。TLS１.1以上のプロトコルに対応していない場合はソフトウェアのアップデート情報をご確認ください。

WINDOWSにおけるSSL3.0の無効化

マイクロソフトからWindowsでSSL3.0を無効化する方法が公開されています。

下記URLに記載されている回避策の「サーバソフトウェア用」を実施してください。

https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

APACHE HTTP SERVERにおけるSSL3.0の無効化

REDHATから Apache Http Server で SSL 3.0 を無効化する方法が公開されています。

下記 URL に記載されている設定変更を実施してください。

https://access.redhat.com/ja/solutions/1232613

HEARTBLEED診断

概要

OpenSSLには、「heartbeat」という機能が有り、ネットワーク機器間で通信がしていない間もTLSセッションの接続を維持し続け、通信相手の存在確認をしています。heartbeatに由来するバグがOpenSSLに混入したのは2011年12月31日のことであり、バグに気付かれないままOpenSSL1.0.1が広く公開されていました。

2014年3月から4月にかけて、Googleのセキュリティーチーム、そしてフィンランドのサイバーセキュリティ会社コデノミコンはOpenSSL 1.0.1シリーズのバグを発見しました。

OpenSSLは、「https://」で始まる、SSL/TLSが動作しているサイトのうち推定6割以上で使用されており、Heartbleedは、OpenSSLを利用しているサーバに細工したデータを送信するだけで、サーバのメモリー上にあるデータ(Webサイトの秘密鍵、ユーザーIDやパスワードや暗号化しているはずのコンテンツ)を、第三者が閲覧できる可能性のあるバグです。

Heartbleedの影響は大きく、この影響を受けたサーバにインストールされているSSLサーバ証明書は、新しい秘密鍵を使って再発行、インストールのやり直しが必要となり、古い証明書の失効手続も必要となります。

診断結果

通信プロトコルが古い為、「Heartbleed」の恐れがあります。SSLで保護されたウェブサイトとブラウザの間で、ハッカーの通信傍受や暗号解読の危険性があります。

解決方法

TLS1.2及び、TLS1.3のプロトコルのみ有効にしてください。OpenSSLをご利用の場合はソフトウェアのアップグレートが必要な場合があります。

証明書の再発行

ウェブサイトで OpenSSL を利用している場合、秘密鍵が既に漏えいしている可能性があります。ウェブサイト運営者は脆弱性の解消後、これまで利用していた証明書を失効させ、新しい秘密鍵を用いて証明書を再取得・再設定する必要があります。

FujiSSLの再発行（無償）：https://www.fujissl.jp/support/reissue/

再発行依頼の際には、これまで使っていた秘密鍵を破棄し、新しく生成した秘密鍵を用いてください。再発行された証明書を対象サーバに設定してください。

中間者攻撃診断

概要

POODLE脆弱性を持つプロトコルでの利用を続けていると、暗号化に必要な鍵を事前に知らない第三者が、大量通信や中間者攻撃によって、暗号化されたデータを解読してしまう危険性があります。

診断結果

脆弱な箇所は見つかりませんでした。

解決方法

証明書の再発行

ウェブサイトで OpenSSL を利用している場合、秘密鍵が既に漏えいしている可能性があります。ウェブサイト運営者は脆弱性の解消後、これまで利用していた証明書を失効させ、新しい秘密鍵を用いて証明書を再取得・再設定する必要があります。

FujiSSLの再発行（無償）：https://www.fujissl.jp/support/reissue/

再発行依頼の際には、これまで使っていた秘密鍵を破棄し、新しく生成した秘密鍵を用いてください。再発行された証明書を対象サーバに設定してください。

Certificate Transparency（証明書の透明性）

概要

CertificateTransparencyとは、日本語で「透かし入り証明書」「証明書の透明性」などと呼ばれています。

CertificateTransparencyは、不正な証明書を早期に発見・検知するための仕組みとして Google 社により考案され、2013 年に「RFC 6962」として規格化されました。 Certificate Transparency は認証局が証明書を発行する都度、全ての証明書発行の証跡を、第三者の監査ログに記載する仕組みです。

それにより利用者が不正に発行された証明書を信頼することを防止します。 Certificate Transparencyはあくまで証明書の信頼性を高めるための追加の仕組みであり、これまでの証明書の検証の仕組みが無くなるわけではありません。

診断結果

Certificate Transparencyが有効になっておりません。

解決方法

証明書の再発行が必要です。：https://www.fujissl.jp/support/reissue/

CAA (Certification Authority Authorization) の確認

概要

CAA レコードは、2013 年 1 月に「RFC6844」として新しく規格化された DNSサーバーで使用するレコードの１つで、意図しない認証局から証明書が発行されることを防ぐ目的で策定されました。

DNS サーバーの CAAレコードに証明書の発行を許可する認証局を
FQDN（ドメイン名を含む）毎に指定することで発行元認証局を限定できます。

診断結果

CAAレコードが設定されておりません。このままでも問題ありませんが、証明書の発行を許可する認証局を指定する事で第三者が別の証明書を発行する事を防ぐ事ができます。

解決方法

証明書の再発行が必要です。：https://www.fujissl.jp/support/reissue/

その他

診断結果

その他情報がありません。

解決方法