SecuAlive

診断 レポート

作成日 2019年8月29日18:49
作成者 ユーザー管理者

診断対象情報

グループ名	デモ用グループ
プロジェクト名	デモ用プロジェクト
サイト名	デモ用プロジェクト
サイトURL	https://demo.tworks.co.jp/mutillidae/

[1] 診断サマリー：暗号スイート確認

開始時間	2019年8月16日11:23
終了時間	2019年8月16日11:23
実行者	TW_管理者
総合評価	A

証明書情報一覧

Port	443/tcp open https		
一般名称(CN)	secualive.jp	発行者一般名称(CN)	RapidSSL RSA CA 2018
組織(O)	-	発行者組織(O)	DigiCert Inc
地域名	-	発行者地域名	-
国名	-	発行者国名	US
署名アルゴリズム	sha256WithRSAEncryption		
公開鍵のタイプ	rsa		
公開鍵長	2048		
発行日	2018-08-28		
有効期限	2019-09-27		

No	危険度	暗号プロトコル	暗号スイート数
1	SSLv2	無効	-
2	SSLv3	無効	-
3	TLSv1.0	A	12
4	TLSv1.1	A	12
5	TLSv1.2	A	24
6	TLSv1.3	無効	-

[1] 暗号スイート一覧

No	暗号スイート	安全度
[A]	TLSv1.0 443/tcp open https	
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(secp256r1)	A
2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(secp256r1)	A
3	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(dh2048)	A
4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(dh2048)	A
5	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(dh2048)	A
6	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(dh2048)	A
7	TLS_RSA_WITH_AES_256_CBC_SHA(rsa2048)	A
8	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(rsa2048)	A
9	TLS_RSA_WITH_AES_128_CBC_SHA(rsa2048)	A
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(rsa2048)	A
11	TLS_DHE_RSA_WITH_SEED_CBC_SHA(dh2048)	A
12	TLS_RSA_WITH_SEED_CBC_SHA(rsa2048)	A
[A]	TLSv1.1 443/tcp open https	
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(secp256r1)	A
2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(secp256r1)	A
3	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(dh2048)	A
4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(dh2048)	A
5	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(dh2048)	A
6	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(dh2048)	A
7	TLS_RSA_WITH_AES_256_CBC_SHA(rsa2048)	A
8	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(rsa2048)	A
9	TLS_RSA_WITH_AES_128_CBC_SHA(rsa2048)	A
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(rsa2048)	A
11	TLS_DHE_RSA_WITH_SEED_CBC_SHA(dh2048)	A
12	TLS_RSA_WITH_SEED_CBC_SHA(rsa2048)	A
[A]	TLSv1.2 443/tcp open https	
1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(secp256r1)	A
2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(secp256r1)	A
3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(secp256r1)	A
4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(secp256r1)	A
5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(secp256r1)	A
6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(secp256r1)	A
7	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(dh2048)	A
8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(dh2048)	A
9	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(dh2048)	A
10	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(dh2048)	A
11	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(dh2048)	A
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(dh2048)	A
13	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(dh2048)	A
14	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(dh2048)	A
15	TLS_RSA_WITH_AES_256_GCM_SHA384(rsa2048)	A
16	TLS_RSA_WITH_AES_256_CBC_SHA256(rsa2048)	A
17	TLS_RSA_WITH_AES_256_CBC_SHA(rsa2048)	A
18	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(rsa2048)	A

19	TLS_RSA_WITH_AES_128_GCM_SHA256(rsa2048)	A
20	TLS_RSA_WITH_AES_128_CBC_SHA256(rsa2048)	A
21	TLS_RSA_WITH_AES_128_CBC_SHA(rsa2048)	A
22	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(rsa2048)	A
23	TLS_DHE_RSA_WITH_SEED_CBC_SHA(dh2048)	A
24	TLS_RSA_WITH_SEED_CBC_SHA(rsa2048)	A

対策参考リンク

No	名前	リンク
1	SSL/TLS暗号設定サーバ設定編	https://www.ipa.go.jp/security/ipg/documents/ssltls_server_config_20150803.pdf
2	SSL/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）	https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
3	Mozilla SSL Configuration Generator	https://mozilla.github.io/server-side-tls/ssl-config-generator/

危険度について

診断で検出された問題は下記の基準で危険度を決定しています。
危険度:HIGH以上は早急な対応が必要になる問題です。

危険度	判定基準
CRITICAL	パスワード漏えい、管理者権限昇格など、システム全体に影響する問題です。 これらの問題が発生する可能性が極めて高く、即日対応する必要があります。
HIGH	情報漏洩や、なりすましなど、ユーザー被害が発生する可能性が高い問題です。 クロスサイトスクリプティングやSQLインジェクションなどの問題があり、インシデント報告やOWASP TOP10などで上位を占めるセキュリティ上の問題です。 このことから、早急に対応する必要があります。
MEDIUM	システムの設定情報や管理情報の漏洩等、システムに対する攻撃手段を提供する可能性がある問題です。 直接被害が発生する可能性は高くないですが、他のセキュリティ上の問題と組み合わさるとレベルが上がる可能性があります。 問題になる可能性があるため対策を検討してください。
LOW	バージョン情報表示や、バナー情報表示など、攻撃者の興味を引く可能性のある問題です。 直接悪用されるよりは、このレベルの情報から攻撃手法を絞っていくことがあります。 予防するうえで対策を検討してください。
INFO	品質やセキュリティのさらなる向上のために弊社が推奨する項目です。

暗号スイート確認の安全度

暗号スイート確認で検出された安全度はA～Fまでの7段階で分けれられています。
A -> F の順に安全度が下がっていきます。
安全度のレベル付は

Qualys SSL Labs Rating Guide - https://www.ssllabs.com/projects/rating-guide/

を参考におこなっています。

暗号スイート確認は

nmap - https://nmap.org/

を利用して行っています。

ご要望、不具合等のご連絡は下記までメール願います。

連絡先	secualive_admin@tworks.co.jp

株式会社トレードワークス