CONFIDENCIAL

SingleID 御中

SingleID Health for FortiGate
結果報告書

2022年3月2日8:23

SingleID

1.目次

2.はじめに

本報告書は、 「2022年3月2日8:02～2022年3月2日8:23」 に実施した脆弱性検査の検査結果についてご報告するものです。

2.1 目的

本検査の目的は、検査対象システムに対してリモートから脆弱性の検査を行い、システムに存在する脆弱性を検出することにあります。 また、脆弱性が検出された場合、そのリスク評価、及び、脆弱性への対策を支援する情報の提供も行います。

3.概要

3.1 検査情報

検査カテゴリ	Basic Network Scan
検査ID	16
検査対象	IP : x.x.x.x Host : x.x.x.x
検査実施日時	2022年3月2日8:02～2022年3月2日8:23

3.2 検査方法

業界トップクラスの広範囲な脆弱性情報を活用し、インターネット経由で、検査対象をリモート診断しました。

3.3 対象者

本報告書は、システムおよびアプリケーション管理者、セキュリティスペシャリスト、監査人、ヘルプデスク、プラットフォームデプロイメント、DevOps担当者を対象としています。

4.検査結果

4.1 ダッシュボード

検査実施日時
2022年3月2日8:02～2022年3月2日8:23
検査対象
IP : x.x.x.x Host : x.x.x.x
検査名
Basic Network Scan

総合　D　判定　大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。

インターネットからアクセス可能な通信ポートごとの診断結果

危険度	重大	高	中	低	情報
443/tcp	1	0	1	0	22
10443/tcp	0	0	0	0	19
80/tcp	0	0	0	0	5

注意

意図しない「インターネットからアクセス可能な通信ポート」が検出されている場合には、機器の設定を見直してください。
特に、ネットワーク機器（ルータ、スイッチ、WiFiアクセスポイント）およびファイアウォール製品の管理コンソール（Web管理GUI、SSH、Telnetなど）を接続元のIPアドレスを制限せずに、インターネットに公開することは推奨されません。

4.2 結果一覧

4.2.1 X.X.X.X

No	検査項目	対象ポート	レベル
1	Fortinet FortiOS SSL VPNのディレクトリトラバーサルの脆弱性（FG-IR-18-384）（直接チェック）	443/tcp	重大
2	弱いハッシュアルゴリズムを使用して署名した SSL 証明書	443/tcp	中
3	サポートされているSSL暗号ブロック連鎖暗号スイート	443/tcp	情報
4	サポートされているSSL暗号ブロック連鎖暗号スイート	10443/tcp	情報
5	SSL Perfect Forward Secrecy暗号スイートがサポートされています	443/tcp	情報
6	SSL Perfect Forward Secrecy暗号スイートがサポートされています	10443/tcp	情報
7	SSL/TLS推奨暗号スイート	443/tcp	情報
8	SSL/TLS推奨暗号スイート	10443/tcp	情報
9	TLSバージョン1.2プロトコルの検出	443/tcp	情報
10	TLSバージョン1.2プロトコルの検出	10443/tcp	情報
11	TLSバージョン1.1プロトコルの検出	443/tcp	情報
12	TLSバージョン1.1プロトコルの検出	10443/tcp	情報
13	サポートされているSSL暗号スイート	443/tcp	情報
14	SSL証明書のcommonNameの不一致	443/tcp	情報
15	SSL証明書のcommonNameの不一致	10443/tcp	情報
16	サポートされているSSL暗号スイート	10443/tcp	情報
17	SSLルート証明機関の証明書情報	443/tcp	情報
18	SSLの自己署名証明書	443/tcp	情報
19	SSLの自己署名証明書	10443/tcp	情報
20	SSL証明書は信頼できません	443/tcp	情報
21	SSL証明書は信頼できません	10443/tcp	情報
22	SSL 証明書チェーンに 2048 ビット未満の RSA 鍵が含まれています	443/tcp	情報
23	SSLの証明書情報	443/tcp	情報
24	SSLの証明書情報	10443/tcp	情報
25	SSLサービスがクライアント証明書を要求する	443/tcp	情報
26	ハイパーテキスト転送プロトコル（HTTP）の情報	10443/tcp	情報
27	ハイパーテキスト転送プロトコル（HTTP）の情報	443/tcp	情報
28	ハイパーテキスト転送プロトコル（HTTP）の情報	80/tcp	情報
29	フォーティネット社のFortiGate Web管理コンソールの検出	10443/tcp	情報
30	互換性のない Strict Transport Security（STS）	443/tcp	情報
31	Strict Transport Security（STS）の検出	443/tcp	情報
32	HTTPSサーバーでHSTSが欠落	10443/tcp	情報

No	検査項目	対象ポート	レベル
33	HTTPサーバーのタイプとバージョン	10443/tcp	情報
34	HTTPサーバーのタイプとバージョン	443/tcp	情報
35	HTTPサーバーのタイプとバージョン	80/tcp	情報
36	Webサーバの404エラーコードをチェックしない	80/tcp	情報
37	許可されるHTTPメソッド（ディレクトリごと）	10443/tcp	情報
38	許可されるHTTPメソッド（ディレクトリごと）	443/tcp	情報
39	サポートされているSSL/TLSバージョン	443/tcp	情報
40	サポートされているSSL/TLSバージョン	10443/tcp	情報
41	サービス検出（HELPリクエスト）	10443/tcp	情報
42	サービス検出	443/tcp	情報
43	サービス検出	80/tcp	情報
44	サービス検出	443/tcp	情報
45	サービス検出	10443/tcp	情報
46	SYNスキャナー	10443/tcp	情報
47	SYNスキャナー	80/tcp	情報
48	SYNスキャナー	443/tcp	情報

4.3 結果詳細

4.3.1

危険度	重大
検査項目	Fortinet FortiOS SSL VPNのディレクトリトラバーサルの脆弱性（FG-IR-18-384）（直接チェック）
対象ポート	443/tcp
説明	リモートホストが、バージョン5.6.8より前のFortiOS 5.6.3か、6.0.5より前のFortiOS 6.0.xを実行しています。したがって、URLのパストラバーサル文字のサニタイズが不適切であるため、SSL VPN Webポータルにあるディレクトリトラバーサルの脆弱性の影響を受けます。認証されていないリモートの攻撃者がこれを悪用し、特別に細工されたHTTPリクエストを介して、任意のFortiOSシステムファイルをダウンロードする可能性があります。
対策	Fortinet FortiOSをバージョン5.6.8、6.0.5、6.2.0、またはそれ以降にアップグレードしてください。
出力	Scanner was able exploit this issue using the following URL : https://x.x.x.x/remote/fgt_lang?lang=/../../../../////////dev/cmdb/sslvpn_websession The string representation of the response from the target host was: 'var fgt_lang = \n\xA7\x18\x18b\0\0\0\0\x01\0\0\0\0\0\0\0\x04\0\0\0\0\0\0\0h\x03\0\0\0\0\0\0\0\0\0\0\x96\x7F\0\0\x01\0\0\0'
VPR	9.9
CVSS v2	5.0（CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N）
CVSS v3	9.8（CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H）
CVE識別番号	CVE-2018-13379

4.3.2

危険度	中
検査項目	弱いハッシュアルゴリズムを使用して署名した SSL 証明書
対象ポート	443/tcp
説明	リモートサービスは、暗号的に弱いハッシュアルゴリズム（MD2、MD4、MD5、SHA1 など）を使って署名された SSL 証明書チェーンを使用します。これらの署名アルゴリズムは、衝突攻撃に脆弱であることが知られています。攻撃者はこれを悪用して、同じデジタル署名の別の証明書を生成し、これによって攻撃者は、影響を受けるサービスになりすますことができます。 このプラグインは、2017年1月1日より後に期限切れとなる、SHA-1で署名したすべてのSSL証明書チェーンを脆弱性として報告します。これは、GoogleがSHA-1暗号ハッシュアルゴリズムを段階的に廃止していくことに従ったものです。 CA データベース（known_CA.inc）に含まれているチェーン内の証明書はすでに無視されていることに注意してください。
対策	SSL 証明書を再発行するには、認証局にお問い合わせください。
出力	The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak. Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiGate/CN=FG100D3G12809591/E=support@fortinet.com Signature Algorithm : SHA-1 With RSA Encryption Valid From : Sep 25 03:25:16 2012 GMT Valid To : Jan 19 03:14:07 2038 GMT Raw PEM certificate : -----BEGIN CERTIFICATE----- MIIDRTCCAi2gAwIBAgIDCNssMA0GCSqGSIb3DQEBBQUAMIGgMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREwDwYDVQQKEwhGb3J0aW5ldDEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MRAwDgYDVQQDEwdzdXBwb3J0MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTAeFw0xMjA5MjUwMzI1MTZaFw0zODAxMTkwMzE0MDdaMIGdMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREwDwYDVQQKEwhGb3J0aW5ldDESMBAGA1UECxMJRm9ydGlHYXRlMRkwFwYDVQQDExBGRzEwMEQzRzEyODA5NTkxMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1jBj3n76ScQXiV6jt9n8fY2QbwibjhcXzsgcrLzq6v/XIYDBMwScIm6j0FcSUjMGWo8roYa0F4FBsc5TCEGynQspcDbM6BKwWxDp3rJfgMmVjFgtaWAc1eTEsp5EXLsl+sWAUG6styKar1EFjxMo4vdadvdV2jCVnoXRP07tZEUCAwEAAaMNMAswCQYDVR0TBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAIqTum04fa5W8Ce+xkTpffWJXwXfBFTLP3BTJOgI2A0sb0+E9QZuWSXn/4+az6/VUi2dXrlW/a64/y6zDx5o5ta0DDlrP2dnGuSd+uIB+7n9gpL1Ire1FKYcvhiVGagz2O65Zi3Tm7b4IskwhPOyKNX0r5OmP45xAxi3cpnfCZ9ZMDISIQ/R0AGZ1LXRUeTwX4zwd9IME81TtyutmIM0zx4g0vCGCC3PhbsIiKgDqrdLVbeAozojG08ZQKTfYje0ptmb4DSwGK7jsBRzoEOAMf30S9ErinsCU852ejMB+aghKOaUAu3ywQaYM+MabPFYVNVLp/ESz/Vss2DB58fO2Rg== -----END CERTIFICATE-----
VPR	6.1
CVSS v2	5.0（CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N）
CVSS v3	7.5（CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N）
CVE識別番号	CVE-2004-2761

4.3.3

危険度	情報
検査項目	サポートされているSSL暗号ブロック連鎖暗号スイート
対象ポート	443/tcp
説明	暗号ブロック連鎖（CBC）モードで動作するSSL暗号の使用が、リモートホストでサポートされます。これらの暗号スイートは、電子コードブック（ECB）モードで追加のセキュリティを提供しますが、不適切に使用すると、情報を漏洩する可能性があります。
対策	該当なし
出力	Here is the list of SSL CBC ciphers supported by the remote server : High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- ECDHE-RSA-CAMELLIA-CBC-128 0xC0, 0x76 ECDH RSA Camellia-CBC(128) SHA256 ECDHE-RSA-CAMELLIA-CBC-256 0xC0, 0x77 ECDH RSA Camellia-CBC(256) SHA384 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1 DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1 CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 DHE-RSA-CAMELLIA128-SHA256 0x00, 0xBE DH RSA Camellia-CBC(128) SHA256 DHE-RSA-CAMELLIA256-SHA256 0x00, 0xC4 DH RSA Camellia-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 RSA-CAMELLIA128-SHA256 0x00, 0xBA RSA RSA Camellia-CBC(128) SHA256 RSA-CAMELLIA256-SHA256 0x00, 0xC0 RSA RSA Camellia-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.4

危険度	情報
検査項目	サポートされているSSL暗号ブロック連鎖暗号スイート
対象ポート	10443/tcp
説明	暗号ブロック連鎖（CBC）モードで動作するSSL暗号の使用が、リモートホストでサポートされます。これらの暗号スイートは、電子コードブック（ECB）モードで追加のセキュリティを提供しますが、不適切に使用すると、情報を漏洩する可能性があります。
対策	該当なし
出力	Here is the list of SSL CBC ciphers supported by the remote server : High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

危険度	情報
検査項目	SSL Perfect Forward Secrecy暗号スイートがサポートされています
対象ポート	443/tcp
説明	リモートホストは、Perfect Forward Secrecy（PFS）暗号化を提供するSSL暗号の使用をサポートします。これらの暗号スイートにより、将来サーバーの秘密鍵が不正にアクセスされた場合に、記録されたSSLトラフィックが解読されないことが保証されます。
対策	該当なし
出力	Here is the list of SSL PFS ciphers supported by the remote server : High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES-128-CCM-AEAD 0xC0, 0x9E DH RSA AES-CCM(128) AEAD DHE-RSA-AES-128-CCM8-AEAD 0xC0, 0xA2 DH RSA AES-CCM8(128) AEAD DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256 DHE-RSA-AES-256-CCM-AEAD 0xC0, 0x9F DH RSA AES-CCM(256) AEAD DHE-RSA-AES-256-CCM8-AEAD 0xC0, 0xA3 DH RSA AES-CCM8(256) AEAD DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384 DHE-RSA-CHACHA20-POLY1305 0xCC, 0xAA DH RSA ChaCha20-Poly1305(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 ECDHE-RSA-CAMELLIA-CBC-128 0xC0, 0x76 ECDH RSA Camellia-CBC(128) SHA256 ECDHE-RSA-CAMELLIA-CBC-256 0xC0, 0x77 ECDH RSA Camellia-CBC(256) SHA384 ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8 ECDH RSA ChaCha20-Poly1305(256) SHA256 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1 DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 DHE-RSA-CAMELLIA128-SHA256 0x00, 0xBE DH RSA Camellia-CBC(128) SHA256 DHE-RSA-CAMELLIA256-SHA256 0x00, 0xC4 DH RSA Camellia-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.6

危険度	情報
検査項目	SSL Perfect Forward Secrecy暗号スイートがサポートされています
対象ポート	10443/tcp
説明	リモートホストは、Perfect Forward Secrecy（PFS）暗号化を提供するSSL暗号の使用をサポートします。これらの暗号スイートにより、将来サーバーの秘密鍵が不正にアクセスされた場合に、記録されたSSLトラフィックが解読されないことが保証されます。
対策	該当なし
出力	Here is the list of SSL PFS ciphers supported by the remote server : High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.7

危険度	情報
検査項目	SSL/TLS推奨暗号スイート
対象ポート	443/tcp
説明	リモートホストに、非推奨の暗号パッケージをアドバタイズする SSL/TLSポートが開いています。次の暗号スイートのサポートのみを有効にすることが推奨されます： TLSv1.3: - 0x13,0x01 TLS_AES_128_GCM_SHA256 - 0x13,0x02 TLS_AES_256_GCM_SHA384 - 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384 これは非常に安全なサービスであり、過去 5 年間（またはそれ以上）にリリースされたほぼすべてのクライアントと互換性があるため、これはサービスの大多数に推奨される構成です。
対策	推奨される暗号スイートのサポートのみを有効にします。

出力	The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below: High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES-128-CCM-AEAD 0xC0, 0x9E DH RSA AES-CCM(128) AEAD DHE-RSA-AES-128-CCM8-AEAD 0xC0, 0xA2 DH RSA AES-CCM8(128) AEAD DHE-RSA-AES-256-CCM-AEAD 0xC0, 0x9F DH RSA AES-CCM(256) AEAD DHE-RSA-AES-256-CCM8-AEAD 0xC0, 0xA3 DH RSA AES-CCM8(256) AEAD DHE-RSA-CHACHA20-POLY1305 0xCC, 0xAA DH RSA ChaCha20-Poly1305(256) SHA256 ECDHE-RSA-CAMELLIA-CBC-128 0xC0, 0x76 ECDH RSA Camellia-CBC(128) SHA256 ECDHE-RSA-CAMELLIA-CBC-256 0xC0, 0x77 ECDH RSA Camellia-CBC(256) SHA384 RSA-AES-128-CCM-AEAD 0xC0, 0x9C RSA RSA AES-CCM(128) AEAD RSA-AES-128-CCM8-AEAD 0xC0, 0xA0 RSA RSA AES-CCM8(128) AEAD RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256 RSA-AES-256-CCM-AEAD 0xC0, 0x9D RSA RSA AES-CCM(256) AEAD RSA-AES-256-CCM8-AEAD 0xC0, 0xA1 RSA RSA AES-CCM8(256) AEAD RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1 DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1 CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 DHE-RSA-CAMELLIA128-SHA256 0x00, 0xBE DH RSA Camellia-CBC(128) SHA256 DHE-RSA-CAMELLIA256-SHA256 0x00, 0xC4 DH RSA Camellia-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 RSA-CAMELLIA128-SHA256 0x00, 0xBA RSA RSA Camellia-CBC(128) SHA256 RSA-CAMELLIA256-SHA256 0x00, 0xC0 RSA RSA Camellia-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.8

危険度	情報
検査項目	SSL/TLS推奨暗号スイート
対象ポート	10443/tcp
説明	リモートホストに、非推奨の暗号パッケージをアドバタイズする SSL/TLSポートが開いています。次の暗号スイートのサポートのみを有効にすることが推奨されます： TLSv1.3: - 0x13,0x01 TLS_AES_128_GCM_SHA256 - 0x13,0x02 TLS_AES_256_GCM_SHA384 - 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256 TLSv1.2: - 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 - 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 - 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 - 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384 - 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 - 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305 - 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 - 0x00,0x9F DHE-RSA-AES256-GCM-SHA384 これは非常に安全なサービスであり、過去 5 年間（またはそれ以上）にリリースされたほぼすべてのクライアントと互換性があるため、これはサービスの大多数に推奨される構成です。
対策	推奨される暗号スイートのサポートのみを有効にします。
出力	The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below: High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.9

危険度	情報
検査項目	TLSバージョン1.2プロトコルの検出
対象ポート	443/tcp
説明	リモートサービスは、TLS1.2を使用して暗号化された接続を受け入れます。
対策	該当なし
出力	TLSv1.2 is enabled and the server supports at least one cipher.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.10

危険度	情報
検査項目	TLSバージョン1.2プロトコルの検出
対象ポート	10443/tcp
説明	リモートサービスは、TLS1.2を使用して暗号化された接続を受け入れます。
対策	該当なし
出力	TLSv1.2 is enabled and the server supports at least one cipher.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.11

危険度	情報
検査項目	TLSバージョン1.1プロトコルの検出
対象ポート	443/tcp
説明	リモートサービスは、TLS1.1を使用して暗号化された接続を受け入れます。 TLS1.1は、最新の推奨されている暗号スイートをサポートしていません。 MAC計算前の暗号化、およびGCMなどの認証された暗号化モードをサポートする暗号は、TLS1.1では使用できません 2020年3月31日以降、TLS1.2以上が有効になっていないエンドポイントは、主要なWebブラウザや主要なベンダーで適切に機能しなくなります。
対策	TLS1.2や1.3のサポートを有効にし、TLS1.1のサポートを無効にしてください。
出力	TLSv1.1 is enabled and the server supports at least one cipher.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.12

危険度	情報
検査項目	TLSバージョン1.1プロトコルの検出
対象ポート	10443/tcp
説明	リモートサービスは、TLS1.1を使用して暗号化された接続を受け入れます。 TLS1.1は、最新の推奨されている暗号スイートをサポートしていません。 MAC計算前の暗号化、およびGCMなどの認証された暗号化モードをサポートする暗号は、TLS1.1では使用できません 2020年3月31日以降、TLS1.2以上が有効になっていないエンドポイントは、主要なWebブラウザや主要なベンダーで適切に機能しなくなります。
対策	TLS1.2や1.3のサポートを有効にし、TLS1.1のサポートを無効にしてください。
出力	TLSv1.1 is enabled and the server supports at least one cipher.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.13

危険度	情報
検査項目	サポートされているSSL暗号スイート
対象ポート	443/tcp
説明	このプラグインは、通信を暗号化するためにリモートサービスでサポートされているSSL暗号を検出します。
対策	該当なし

出力	Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES-128-CCM-AEAD 0xC0, 0x9E DH RSA AES-CCM(128) AEAD DHE-RSA-AES-128-CCM8-AEAD 0xC0, 0xA2 DH RSA AES-CCM8(128) AEAD DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256 DHE-RSA-AES-256-CCM-AEAD 0xC0, 0x9F DH RSA AES-CCM(256) AEAD DHE-RSA-AES-256-CCM8-AEAD 0xC0, 0xA3 DH RSA AES-CCM8(256) AEAD DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384 DHE-RSA-CHACHA20-POLY1305 0xCC, 0xAA DH RSA ChaCha20-Poly1305(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 ECDHE-RSA-CAMELLIA-CBC-128 0xC0, 0x76 ECDH RSA Camellia-CBC(128) SHA256 ECDHE-RSA-CAMELLIA-CBC-256 0xC0, 0x77 ECDH RSA Camellia-CBC(256) SHA384 ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8 ECDH RSA ChaCha20-Poly1305(256) SHA256 RSA-AES-128-CCM-AEAD 0xC0, 0x9C RSA RSA AES-CCM(128) AEAD RSA-AES-128-CCM8-AEAD 0xC0, 0xA0 RSA RSA AES-CCM8(128) AEAD RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256 RSA-AES-256-CCM-AEAD 0xC0, 0x9D RSA RSA AES-CCM(256) AEAD RSA-AES-256-CCM8-AEAD 0xC0, 0xA1 RSA RSA AES-CCM8(256) AEAD RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1 DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1 CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 DHE-RSA-CAMELLIA128-SHA256 0x00, 0xBE DH RSA Camellia-CBC(128) SHA256 DHE-RSA-CAMELLIA256-SHA256 0x00, 0xC4 DH RSA Camellia-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 RSA-CAMELLIA128-SHA256 0x00, 0xBA RSA RSA Camellia-CBC(128) SHA256 RSA-CAMELLIA256-SHA256 0x00, 0xC0 RSA RSA Camellia-CBC(256) SHA256 SSL Version : TLSv11 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1 DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1 CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	

CVSS v2	
CVSS v3	
CVE識別番号	

4.3.14

危険度	情報
検査項目	SSL証明書のcommonNameの不一致
対象ポート	443/tcp
説明	このサービスから提示された SSL証明書の「commonName」（CN）が、サービスがリッスンするホスト名と一致しません。
対策	マシンに複数の名前がある場合は、ユーザーが証明書に記載されている共通名に一致する DNS ホスト名を通してサービスに接続されていることを、確認してください。
出力	The host name known by Scanner is : x.x.x.x The Common Name in the certificate is : fg100d3g12809591
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.15

危険度	情報
検査項目	SSL証明書のcommonNameの不一致
対象ポート	10443/tcp
説明	このサービスから提示された SSL証明書の「commonName」（CN）が、サービスがリッスンするホスト名と一致しません。
対策	マシンに複数の名前がある場合は、ユーザーが証明書に記載されている共通名に一致する DNS ホスト名を通してサービスに接続されていることを、確認してください。
出力	The host name known by Scanner is : x.x.x.x The Common Name in the certificate is : fg100d3g12809591
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.16

危険度	情報
検査項目	サポートされているSSL暗号スイート
対象ポート	10443/tcp
説明	このプラグインは、通信を暗号化するためにリモートサービスでサポートされているSSL暗号を検出します。
対策	該当なし
出力	Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256 DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 SSL Version : TLSv11 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1 DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.17

危険度	情報
検査項目	SSLJルート証明機関の証明書情報
対象ポート	443/tcp
説明	リモートサービスは、チェーンの最上位に自己署名ルート証明機関証明書を含むSSL証明書チェーンを使用します。
対策	このルート証明機関の証明書の使用が、組織の利用規定およびセキュリティポリシーに準拠していることを確認してください。
出力	The following root Certification Authority certificate was found : |-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/E=support@fortinet.com |-Issuer : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/E=support@fortinet.com |-Valid From : Jul 16 22:34:39 2015 GMT |-Valid To : Jan 19 22:34:39 2038 GMT |-Signature Algorithm : SHA-256 With RSA Encryption
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.18

危険度	情報
検査項目	SSLの自己署名証明書
対象ポート	443/tcp
説明	このサービスのX.509証明書チェーンが、広く認められている認証局によって署名されていません。リモートホストが稼働中のパブリックホストの場合、誰でもリモートホストに対して中間者攻撃を確立できるため、SSLを使用する価値がなくなります。 このプラグインは、自己署名ではない、正当に認められていない認証局によって署名された証明書にすぎない証明書チェーンを、チェックしないことに、注意してください。
対策	このサービス用の適切なSSL証明書を購入または生成します。
出力	The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities : |-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/E=support@fortinet.com
VPR	
CVSS v2	6.4（CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N）
CVSS v3	
CVE識別番号	

4.3.19

危険度	情報
検査項目	SSLの自己署名証明書
対象ポート	10443/tcp
説明	このサービスのX.509証明書チェーンが、広く認められている認証局によって署名されていません。リモートホストが稼働中のパブリックホストの場合、誰でもリモートホストに対して中間者攻撃を確立できるため、SSLを使用する価値がなくなります。 このプラグインは、自己署名ではない、正当に認められていない認証局によって署名された証明書にすぎない証明書チェーンを、チェックしないことに、注意してください。
対策	このサービス用の適切なSSL証明書を購入または生成します。
出力	The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities : |-Subject : O=Fortinet Ltd./CN=FG100D3G12809591
VPR	
CVSS v2	6.4（CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N）
CVSS v3	
CVE識別番号	

危険度	情報
検査項目	SSL証明書は信頼できません
対象ポート	443/tcp
説明	サーバーの X.509 証明書は信頼できません。以下に説明するように、この状況は3つの異なる経緯で発生する可能性があり、これによって信頼チェーンが破損する可能性があります。 - まず、サーバーから送信された、証明書チェーンの最上位の証明書が、既知の公共認証期間由来のものではない可能性があります。これは、チェーンの最上位が正当に認められていない自己署名証明書であるか、または証明書チェーンの最上位と既知の公共認証機関とをつなぐ中間の証明書が見つからない場合に起こることがあります。 - 2 番目に、スキャンする時点で有効でない証明書が証明書チェーンに含まれていることがあります。これは、証明書の「notBefore」（有効期限の開始日時）日付よりも前または「notAfter」（有効期限の終了日時）日付よりも後にスキャンが実行された場合に起こることがあります。 - 3 番目に、証明書チェーンに、証明書の情報と一致しなかった署名が含まれているか、検証できなかった署名が含まれている可能性があります。署名が不適切な場合、不適切な署名が含まれている証明書に発行者が再度署名することで修正できます。証明書を検証できなかった場合、その原因は、証明書の発行者が、 Scanner がサポートしていないか認識しない署名アルゴリズムを使用したことにあります。 リモートホストが稼働時の公開ホストの場合、証明書チェーンの切断により、ユーザーが Web サーバーの信憑性と ID を検証するのがより困難になります。これにより、リモートホストに対して中間者攻撃を実行することがより簡単になることがあります。
対策	このサービス用の適切なSSL証明書を購入または生成します。
出力	The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/E=support@fortinet.com |-Issuer : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=support/E=support@fortinet.com
VPR	
CVSS v2	6.4（CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N）
CVSS v3	6.5（CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N）
CVE識別番号	

4.3.21

危険度	情報
検査項目	SSL証明書は信頼できません
対象ポート	10443/tcp
説明	サーバーの X.509 証明書は信頼できません。以下に説明するように、この状況は3つの異なる経緯で発生する可能性があり、これによって信頼チェーンが破損する可能性があります。 - まず、サーバーから送信された、証明書チェーンの最上位の証明書が、既知の公共認証期間由来のものではない可能性があります。これは、チェーンの最上位が正当に認められていない自己署名証明書であるか、または証明書チェーンの最上位と既知の公共認証機関とをつなぐ中間の証明書が見つからない場合に起こることがあります。 - 2 番目に、スキャンする時点で有効でない証明書が証明書チェーンに含まれていることがあります。これは、証明書の「notBefore」（有効期限の開始日時）日付よりも前または「notAfter」（有効期限の終了日時）日付よりも後にスキャンが実行された場合に起こることがあります。 - 3 番目に、証明書チェーンに、証明書の情報と一致しなかった署名が含まれているか、検証できなかった署名が含まれている可能性があります。署名が不適切な場合、不適切な署名が含まれている証明書に発行者が再度署名することで修正できます。証明書を検証できなかった場合、その原因は、証明書の発行者が、 Scanner がサポートしていないか認識しない署名アルゴリズムを使用したことにあります。 リモートホストが稼働時の公開ホストの場合、証明書チェーンの切断により、ユーザーが Web サーバーの信憑性と ID を検証するのがより困難になります。これにより、リモートホストに対して中間者攻撃を実行することがより簡単になることがあります。
対策	このサービス用の適切なSSL証明書を購入または生成します。
出力	The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : O=Fortinet Ltd./CN=FG100D3G12809591 |-Issuer : O=Fortinet Ltd./CN=FG100D3G12809591
VPR	
CVSS v2	6.4（CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N）
CVSS v3	6.5（CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N）
CVE識別番号	

4.3.22

危険度	情報
検査項目	SSL 証明書チェーンに 2048 ビット未満の RSA 鍵が含まれています
対象ポート	443/tcp
説明	リモートホストによって送信された 1 つ以上の X.509 証明書に、2048 ビットより短い鍵が含まれています。認証局/ブラウザ（CA/B）フォーラムが策定した業界標準によると、2014 年 1 月 1 日以降に発行された証明書では 2048 ビット以上の必要があります。 一部のブラウザ SSL 実装は、2014 年 1 月 1 日以降、2048 ビット未満の鍵を拒否することがあります。さらに、一部の SSL 証明書ベンダーは、2014 年 1 月 1 日より前に発行された 2048 ビット未満の証明書を無効にすることがあります。 本セキュリティ診断は、2048 ビット未満の RSA 鍵が含まれているルート証明書が 2010 年 12 月 31 日より前に発行されている場合、その証明書をフラグしないことに、注意してください（標準により、適用外と見なされるため）。
対策	長さが 2048 ビット未満の RSA 鍵が含まれているチェーン内の証明書を、より長い鍵の証明書で置き換えて、古い証明書で署名された証明書を再発行してください。
出力	The following certificates were part of the certificate chain sent by the remote host, but contain RSA keys that are considered to be weak : |-Subject : C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=FortiGate/CN=FG100D3G12809591/E=support@fortinet.com |-RSA Key Length : 1024 bits
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.23

危険度	情報
検査項目	SSLの証明書情報
対象ポート	443/tcp
説明	このプラグインは、すべてのSSL関連ポートに接続し、X.509証明書を抽出してダンプしようとします。
対策	該当なし

出力

Subject Name:

Country: US
State/Province: California
Locality: Sunnyvale
Organization: Fortinet
Organization Unit: FortiGate
Common Name: FG100D3G12809591
Email Address: support@fortinet.com

Issuer Name:

Country: US
State/Province: California
Locality: Sunnyvale
Organization: Fortinet
Organization Unit: Certificate Authority
Common Name: support
Email Address: support@fortinet.com

Serial Number: 08 DB 2C

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 25 03:25:16 2012 GMT
Not Valid After: Jan 19 03:14:07 2038 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 30 63 DE 7E FA 49 C4 17 89 5E A3 B7 D9 FC 7D 8D 90 6F
08 9B 8E 17 17 CE C8 1C AC BC EA EA FF D7 21 80 C1 33 04 9C
22 6E A3 D0 57 12 52 33 06 5A 8F 2B A1 86 B4 17 81 41 B1 CE
53 08 41 B2 9D 0B 29 70 36 CC E8 12 B0 5B 10 E9 DE B2 5F 80
C9 95 8C 58 2D 69 60 1C D5 E4 C4 B2 9E 44 5C BB 25 FA C5 80
50 6E AC B7 22 9A AF 51 05 8F 13 28 E2 F7 5A 76 F7 55 DA 30
95 9E 85 D1 3F 4E ED 64 45
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 22 A4 EE 9B 4E 1F 6B 95 BC 09 EF B1 91 3A 5F 7D 62 57 C1
77 C1 15 32 CF DC 14 C9 3A 02 36 03 4B 1B D3 E1 3D 41 9B 96
49 79 FF E3 E6 B3 EB F5 54 8B 67 57 AE 55 BF 6B AE 3F CB AC
C3 C7 9A 39 B5 AD 03 0E 5A CF D9 D9 C6 B9 27 7E B8 80 7E EE
7F 60 A4 BD 48 AD ED 45 29 87 2F 86 25 46 6A 0C F6 3B AE 59
8B 74 E6 ED BE 08 B2 4C 21 3C EC 8A 35 7D 2B E4 E9 8F E3 9C
40 C6 2D DC A6 77 C2 67 D6 4C 0E 54 88 43 F4 74 00 66 75 2D
74 54 79 3C 17 E3 3C 1D F4 83 04 F3 54 ED CA EB 66 20 CD 33
C7 88 34 BC 21 82 0B 73 E1 6E C2 22 2A 00 EA AD D2 D5 6D E0
28 CE 88 C6 D3 C6 50 29 37 D8 8D ED 29 B6 66 F8 0D 2C 06 2B
B8 EC 05 1C E8 10 E0 0C 7F 7D 12 F4 4A E2 9E C0 94 F3 9D 9E
8C C0 7E 6A 08 4A 39 A5 00 BB 7C B0 41 A6 0C F8 C6 9B 3C 56
15 35 52 E9 FC 44 B3 FD 5B 2C D8 30 79 F1 F3 B6 46

Extension: Basic Constraints (2.5.29.19)
Critical: 0

Fingerprints :

SHA-256 Fingerprint: B6 FC B2 C4 A8 4E E1 ED 65 4D 82 F9 A1 2F F7 CE 4A 1D 22 39
C9 56 1E 15 67 60 4E 23 5D F4 BB 57
SHA-1 Fingerprint: 91 54 44 D0 1E 87 14 B6 B3 4A A8 9D 87 F0 24 09 E4 C2 AA EA
MD5 Fingerprint: A5 7B DD 0E B3 66 1C 8F 8A 03 C5 3B 9F 4B FF 4E

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDRTCCAi2gAwIBAgIDCNssMA0GCSqGSIb3DQEBBQUAMIGgMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm
5pYTESMBAGA1UEBxMJU3Vubnl2YWxlMREwDwYDVQQKEwhGb3J0aW5ldDEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV
0aG9yaXR5MRAwDgYDVQQDEwdzdXBwb3J0MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTAeFw0xMjA
5MjUwMzI1MTZaFw0zODAxMTkwMzE0MDdaMIGdMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBA
GA1UEBxMJU3Vubnl2YWxlMREwDwYDVQQKEwhGb3J0aW5ldDESMBAGA1UECxMJRm9ydGlHYXRlMRkwFwYDVQQDExBGRz
EwMEQzRzEyODA5NTkxMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGZvcnRpbmV0LmNvbTCBnzANBgkqhkiG9w0BAQEFAAO
BjQAwgYkCgYEA1jBj3n76ScQXiV6jt9n8fY2QbwibjhcXzsgcrLzq6v/XIYDBMwScIm6j0FcSUjMGWo8roYa0F4FBsc5TCEGynQspcD
bM6BKwWxDp3rJfgMmVjFgtaWAc1eTEsp5EXLsl+sWAUG6styKar1EFjxMo4vdadvdV2jCVnoXRP07tZEUCAwEAAaMNMAswCQ
YDVR0TBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAIqTum04fa5W8Ce+xkTpffWJXwXfBFTLP3BTJOgI2A0sb0+E9QZuWSXn/4
+az6/VUi2dXrlW/a64/y6zDx5o5ta0DDlrP2dnGuSd+uIB+7n9gpL1Ire1FKYcvhiVGagz2O65Zi3Tm7b4IskwhPOyKNX0r5OmP45x

	Axi3cpnfCZ9ZMDISIQ/R0AGZ1LXRUeTwX4zwd9IME81TtyutmIM0zx4g0vCGCC3PhbsIiKgDqrdLVbeAozojG08ZQKTfYje0ptmb4 DSwGK7jsBRzoEOAMf30S9ErinsCU852ejMB+aghKOaUAu3ywQaYM+MabPFYVNVLp/ESz/Vss2DB58fO2Rg== -----END CERTIFICATE-----
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.24

危険度	情報
検査項目	SSLの証明書情報
対象ポート	10443/tcp
説明	このプラグインは、すべてのSSL関連ポートに接続し、X.509証明書を抽出してダンプしようとします。
対策	該当なし

出力

Subject Name:

Organization: Fortinet Ltd.
Common Name: FG100D3G12809591

Issuer Name:

Organization: Fortinet Ltd.
Common Name: FG100D3G12809591

Serial Number: 2F 7B 9E 21 61 17 3E 76

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 03 05:13:20 2022 GMT
Not Valid After: Feb 04 05:13:20 2032 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 EC 49 F4 9D 58 A5 B5 C7 90 70 ED 82 86 E1 14 F0 A0 14 8B
0D 49 F7 78 FC FA B1 BD 04 CB A4 47 66 97 EC FC 65 A3 08 E8
20 EB A7 41 21 2E BE AF 28 CC DC C5 FA 58 EA 64 41 47 A0 AE
B1 EF 60 0C D4 9E EB 7D 4E 33 D0 F9 21 FC 73 A0 F2 07 DC 56
B7 6B 52 97 90 74 B7 4B 04 50 DF 79 99 DA 96 37 55 99 A8 B4
CB 15 84 D3 F2 96 4B 27 F6 99 11 9A F0 9C CB 72 B0 4A C3 6A
AB E6 B7 84 C9 E1 76 85 05 06 B4 A8 B1 34 43 01 9D 58 B3 76
D0 F3 B0 C3 77 AD AC 93 0C 57 62 A7 63 53 CE 3C 4E 9D 93 D6
A8 F6 AA F1 70 3D D8 19 41 06 F6 7D B3 B1 91 0B DF ED 94 E9
9E 0E 57 D3 BD 17 E0 FD 66 7C 56 1B 5C DD 45 DF 3A F1 D8 03
7D 05 08 E7 20 E5 58 37 EF 22 DC D9 1B CC EE B1 2E A7 2F 40
9C EE AE 7E 07 5C 52 DF 7E 34 53 D3 D4 CE DA 88 11 D8 A4 AF
50 0E 57 47 B3 F5 EF 84 70 FE 60 00 DC F2 C1 01 8D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 92 84 DE 69 82 1C 02 BE 6A C3 C3 73 90 66 81 46 8A E5 2D
45 38 AB 49 7D 9C A3 A6 38 E2 6B E6 B5 99 96 C9 47 7A DC 66
E5 A1 50 83 D5 80 5D 12 F0 72 EA 92 1E AF 04 44 9D AA 97 62
33 FF 80 1B 61 4A AC 7F 1D E3 C0 B2 12 5A 9E F1 D4 62 CF 63
CA 23 63 34 37 E6 82 90 CE F0 D3 41 A5 DB 53 3E 20 84 09 A3
3B CA 3B 2D A8 49 53 9A 57 2F 3A 14 F1 F4 7E 5D CC 4F 54 5C
45 3C A3 F5 0B 11 84 6C B3 96 EC 3A 93 53 EF 77 DA B9 2D BE
1F B4 12 2F 26 F5 90 2F EA 4E 5F 61 67 58 18 0F FB BC B6 23
32 86 CE 1E DC 05 0A 46 BF 9F E5 77 CC 16 6B 7F 4E A0 1C E9
7F 26 0F D3 88 B6 7B 12 D8 B7 84 F0 07 F8 87 84 B6 05 06 9C
99 7D 7F DD F6 D7 6A 20 54 4A 8D E7 CB 89 16 93 07 C6 73 C7
4F 2D 96 F1 B5 62 74 A9 66 9A F0 9A DC CC 93 5D BD C3 34 02
EC 77 3A 1E 7B D1 C4 39 0A 1F 5E D7 6D CB 9A 87 66

Extension: Basic Constraints (2.5.29.19)
Critical: 0

Fingerprints :

SHA-256 Fingerprint: 50 18 5E 11 A9 03 30 B3 DA 1A D4 6F 10 52 3B 4C 57 36 22 93
8B FA 8F 23 33 60 66 F9 AD 05 FC 50
SHA-1 Fingerprint: 52 48 49 E0 5B B1 1E 9B F2 42 59 4F F3 A0 70 80 19 F7 19 08
MD5 Fingerprint: 89 94 8D F3 32 D6 36 B3 2E 49 87 3E 38 7C 3A 18

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIC9TCCAd2gAwIBAgIIL3ueIWEXPnYwDQYJKoZIhvcNAQELBQAwMzEWMBQGA1UECgwNRm9ydGluZXQgTHRkLjEZMBcGA
1UEAwwQRkcxMDBEM0cxMjgwOTU5MTAeFw0yMjAyMDMwNTEzMjBaFw0zMjAyMDQwNTEzMjBaMDMxFjAUBgNVBAoMD
UZvcnRpbmV0IEx0ZC4xGTAXBgNVBAMMEEZHMTAwRDNHMTI4MDk1OTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggE
KAoIBAQDsSfSdWKW1x5Bw7YKG4RTwoBSLDUn3ePz6sb0Ey6RHZpfs/GWjCOgg66dBIS6+ryjM3MX6WOpkQUegrrHvYAzUnu
t9TjPQ+SH8c6DyB9xWt2tSl5B0t0sEUN95mdqWN1WZqLTLFYTT8pZLJ/aZEZrwnMtysErDaqvmt4TJ4XaFBQa0qLE0QwGdWLN
20POww3etrJMMV2KnY1POPE6dk9ao9qrxcD3YGUEG9n2zsZEL3+2U6Z4OV9O9F+D9ZnxWG1zdRd868dgDfQUI5yDlWDfvItz
ZG8zusS6nL0Cc7q5+B1xS3340U9PUztqIEdikr1AOV0ez9e+EcP5gANzywQGNAgMBAAGjDTALMAkGA1UdEwQCMAAwDQYJK
oZIhvcNAQELBQADggEBAJKE3mmCHAK+asPDc5BmgUaK5S1FOKtJfZyjpjjia+a1mZbJR3rcZuWhUIPVgF0S8HLqkh6vBESdqpd
iM/+AG2FKrH8d48CyElqe8dRiz2PKI2M0N+aCkM7w00Gl21M+IlQJozvKOy2oSVOaVy86FPH0fl3MT1RcRTyj9QsRhGyzluw6k1P
vd9q5Lb4ftBlvJvWQL+pOX2FnWBgP+7y2lzKGzh7cBQpGv5/ld8wWa39OoBzpfyYP04i2exLYt4TwB/iHhLYFBpyZfX/d9tdqIFRKje
fLiRaTB8Zzx08tlvG1YnSpZprwmtzMk129wzQC7Hc6HnvRxDkKH17Xbcuah2Y=
-----END CERTIFICATE-----

VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.25

危険度	情報
検査項目	SSLサービスがクライアント証明書を要求する
対象ポート	443/tcp
説明	リモートサービスはSSL / TLSを使用して通信を暗号化し、クライアント証明書を要求し、基盤となるサービスへの接続を確立するために有効な証明書を必要とする場合があります。
対策	該当なし
出力	A TLSv11/TLSv12 server is listening on this port that requests a client certificate.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

危険度	情報
検査項目	ハイパーテキスト転送プロトコル（HTTP）の情報
対象ポート	10443/tcp
説明	このテストにより、リモートHTTPプロトコルに関する一部の情報（使用するバージョン、HTTPキープアライブおよびHTTPパイプライン方式が有効であるか、など）が提供されます。 このテストは情報提供のみであり、セキュリティ問題は示しません。
対策	該当なし
出力	Response Code : HTTP/1.1 200 OK Protocol version : HTTP/1.1 SSL : yes Keep-Alive : yes Options allowed : GET, HEAD, OPTIONS Headers : Date: Tue, 01 Mar 2022 23:09:14 GMT Server: xxxxxxxx-xxxxx Vary: Accept-Encoding Content-Length: 79 Keep-Alive: timeout=10, max=18 Connection: Keep-Alive Content-Type: text/html; charset=utf-8 X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block X-UA-Compatible: IE=Edge Response Body : <html> <script language=javascript> top.location="/login"; </script> </html>
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.27

危険度	情報
検査項目	ハイパーテキスト転送プロトコル（HTTP）の情報
対象ポート	443/tcp
説明	このテストにより、リモートHTTPプロトコルに関する一部の情報（使用するバージョン、HTTPキープアライブおよびHTTPパイプライン方式が有効であるか、など）が提供されます。 このテストは情報提供のみであり、セキュリティ問題は示しません。
対策	該当なし
出力	Response Code : HTTP/1.1 200 OK Protocol version : HTTP/1.1 SSL : yes Keep-Alive : yes Options allowed : GET, HEAD, OPTIONS Headers : Date: Tue, 01 Mar 2022 23:09:14 GMT Server: xxxxxxxx-xxxxx Last-Modified: Thu, 13 Sep 2018 19:25:00 GMT ETag: "83-5b9ab98c" Accept-Ranges: bytes Content-Length: 131 Keep-Alive: timeout=10, max=100 Connection: Keep-Alive Content-Type: text/html X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 Response Body : <html><script type="text/javascript"> if (window!=top) top.location=window.location;top.location="/remote/login"; </script></html>
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.28

危険度	情報
検査項目	ハイパーテキスト転送プロトコル（HTTP）の情報
対象ポート	80/tcp
説明	このテストにより、リモートHTTPプロトコルに関する一部の情報（使用するバージョン、HTTPキープアライブおよびHTTPパイプライン方式が有効であるか、など）が提供されます。 このテストは情報提供のみであり、セキュリティ問題は示しません。
対策	該当なし
出力	Response Code : HTTP/1.1 302 Found Protocol version : HTTP/1.1 SSL : no Keep-Alive : yes Options allowed : (Not implemented) Headers : Date: Tue, 01 Mar 2022 23:09:14 GMT Server: xxxxxxxx-xxxxx Location: https://x.x.x.x:10443/ Keep-Alive: timeout=10, max=17 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=iso-8859-1 X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block X-UA-Compatible: IE=Edge Response Body : <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>302 Found</TITLE> </HEAD><BODY> <H1>Found</H1> The document has moved <A HREF="https://x.x.x.x:10443/">here</A>.<P> </BODY></HTML>
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.29

危険度	情報
検査項目	フォーティネット社のFortiGate Web管理コンソールの検出
対象ポート	10443/tcp
説明	フォーティネット社のFortiGateファイアウォールがリモートホストで実行されており、Webベースの管理コンソールポートへの接続が許可されています。 このソフトウェアを使用していることを攻撃者に知らせると、攻撃者が、集中的に攻撃したり、戦略を変更したりするのに役立ちます。これに加えて、攻撃者はリモートインターフェイスに対してブルートフォース攻撃を仕掛ける可能性があります。
対策	このポートへの着信トラフィックをフィルタリングします。
出力	The following instance of FortiOS Web Interface was detected on the remote host : Version : >= 5.4 URL : https://x.x.x.x:10443/
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.30

危険度	情報
検査項目	互換性のない Strict Transport Security（STS）
対象ポート	443/tcp
説明	リモート Web サーバーに Strict Transport Security が不適切に実装されています。
対策	該当なし
出力	The response from the web server listening on port 80 : - does not contain a Status-Code of 301.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.31

危険度	情報
検査項目	Strict Transport Security（STS）の検出
対象ポート	443/tcp
説明	リモートWebサーバーはStrictTransport Security（STS）を実装しています。 STSの目的は、ユーザーが誤ってブラウザのセキュリティをダウングレードしないようにすることです。 暗号化されていないすべてのHTTP接続はHTTPSにリダイレクトされます。ブラウザは、すべてのCookieを「安全」として扱い、安全でない可能性のある状況が発生した場合に接続を閉じることが期待されています。
対策	該当なし
出力	The STS header line is : Strict-Transport-Security: max-age=31536000
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.32

危険度	情報
検査項目	HTTPSサーバーでHSTSが欠落
対象ポート	10443/tcp
説明	リモートのHTTPSサーバーが、HTTP Strict Transport Security（HSTS）を強制していません。HSTSは、HTTPS経由でのみ通信するようにブラウザに指示するためにサーバー上で構成できる、オプションの応答ヘッダーです。HSTSがないことにより、ダウングレード攻撃、SSL-stripping中間者攻撃が可能になり、クッキーのハイジャックに対する保護が弱体化します。
対策	リモートWebサーバーをHSTSを使用するように設定します。
出力	The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.33

危険度	情報
検査項目	HTTPサーバーのタイプとバージョン
対象ポート	10443/tcp
説明	このプラグインは、リモートWebサーバのタイプとバージョンを判別しようとします。
対策	該当なし
出力	The remote web server type is : xxxxxxxx-xxxxx
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.34

危険度	情報
検査項目	HTTPサーバーのタイプとバージョン
対象ポート	443/tcp
説明	このプラグインは、リモートWebサーバのタイプとバージョンを判別しようとします。
対策	該当なし
出力	The remote web server type is : xxxxxxxx-xxxxx
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.35

危険度	情報
検査項目	HTTPサーバーのタイプとバージョン
対象ポート	80/tcp
説明	このプラグインは、リモートWebサーバのタイプとバージョンを判別しようとします。
対策	該当なし
出力	The remote web server type is : xxxxxxxx-xxxxx
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.36

危険度	情報
検査項目	Webサーバの404エラーコードをチェックしない
対象ポート	80/tcp
説明	リモートWebサーバーは、存在しないファイルが要求されたときに「404 Not Found」エラーコードを返さないように構成されています。おそらく、代わりにサイトマップ、検索ページ、または認証ページを返します。 Scannerは、これに対するいくつかの対策を有効にしました。ただし、不十分な場合があります。このポートに多数のセキュリティホールが生成された場合、それらすべてが正確であるとは限りません。
対策	該当なし
出力	CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was : http://x.x.x.x/HsoABtmfIA_k.html
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.37

危険度	情報
検査項目	許可されるHTTPメソッド（ディレクトリごと）
対象ポート	10443/tcp
説明	
対策	該当なし
出力	Based on the response to an OPTIONS request : - HTTP methods HEAD OPTIONS GET are allowed on : /
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.38

危険度	情報
検査項目	許可されるHTTPメソッド（ディレクトリごと）
対象ポート	443/tcp
説明	
対策	該当なし
出力	Based on the response to an OPTIONS request : - HTTP methods HEAD OPTIONS GET are allowed on : /
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.39

危険度	情報
検査項目	サポートされているSSL/TLSバージョン
対象ポート	443/tcp
説明	このプラグインは、通信を暗号化するためにリモートサービスでサポートされているSSLおよびTLSのバージョンを検出します。
対策	該当なし
出力	This port supports TLSv1.1/TLSv1.2.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.40

危険度	情報
検査項目	サポートされているSSL/TLSバージョン
対象ポート	10443/tcp
説明	このプラグインは、通信を暗号化するためにリモートサービスでサポートされているSSLおよびTLSのバージョンを検出します。
対策	該当なし
出力	This port supports TLSv1.1/TLSv1.2.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.41

危険度	情報
検査項目	サービス検出（HELPリクエスト）
対象ポート	10443/tcp
説明	バナーによって、または「HELP」リクエストを受け取った際に送信するエラーメッセージを見ることで、リモートサービスを識別できました。
対策	該当なし
出力	A web server seems to be running on this port.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.42

危険度	情報
検査項目	サービス検出
対象ポート	443/tcp
説明	本セキュリティ診断は、バナーによって、またはHTTPリクエストを受信したときに送信するエラーメッセージを確認することで、リモートサービスを識別できました。
対策	該当なし
出力	A web server is running on this port through TLSv1.2.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.43

危険度	情報
検査項目	サービス検出
対象ポート	80/tcp
説明	本セキュリティ診断は、バナーによって、またはHTTPリクエストを受信したときに送信するエラーメッセージを確認することで、リモートサービスを識別できました。
対策	該当なし
出力	A web server is running on this port.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.44

危険度	情報
検査項目	サービス検出
対象ポート	443/tcp
説明	本セキュリティ診断は、バナーによって、またはHTTPリクエストを受信したときに送信するエラーメッセージを確認することで、リモートサービスを識別できました。
対策	該当なし
出力	A TLSv1.2 server answered on this port.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.45

危険度	情報
検査項目	サービス検出
対象ポート	10443/tcp
説明	本セキュリティ診断は、バナーによって、またはHTTPリクエストを受信したときに送信するエラーメッセージを確認することで、リモートサービスを識別できました。
対策	該当なし
出力	A TLSv1.1 server answered on this port.
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.46

危険度	情報
検査項目	SYNスキャナー
対象ポート	10443/tcp
説明	このプラグインは、SYN「ハーフオープン」ポートスキャナーです。ファイアウォールで保護されたターゲットに対しても、適度な速さを維持する必要があります。 SYNスキャンは、破損したサービスに対するTCP（フル接続）スキャンより煩わしくありませんが、ネットワークに負荷がかかっている場合に、ファイアウォールの堅牢性を低下させるという問題を引き起こしたり、リモートターゲットで接続をオープンのまま残したりする可能性があります。
対策	IPフィルターでターゲットを保護します。
出力	Port 10443/tcp was found to be open
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.47

危険度	情報
検査項目	SYNスキャナー
対象ポート	80/tcp
説明	このプラグインは、SYN「ハーフオープン」ポートスキャナーです。ファイアウォールで保護されたターゲットに対しても、適度な速さを維持する必要があります。 SYNスキャンは、破損したサービスに対するTCP（フル接続）スキャンより煩わしくありませんが、ネットワークに負荷がかかっている場合に、ファイアウォールの堅牢性を低下させるという問題を引き起こしたり、リモートターゲットで接続をオープンのまま残したりする可能性があります。
対策	IPフィルターでターゲットを保護します。
出力	Port 80/tcp was found to be open
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

4.3.48

危険度	情報
検査項目	SYNスキャナー
対象ポート	443/tcp
説明	このプラグインは、SYN「ハーフオープン」ポートスキャナーです。ファイアウォールで保護されたターゲットに対しても、適度な速さを維持する必要があります。 SYNスキャンは、破損したサービスに対するTCP（フル接続）スキャンより煩わしくありませんが、ネットワークに負荷がかかっている場合に、ファイアウォールの堅牢性を低下させるという問題を引き起こしたり、リモートターゲットで接続をオープンのまま残したりする可能性があります。
対策	IPフィルターでターゲットを保護します。
出力	Port 443/tcp was found to be open
VPR	
CVSS v2	
CVSS v3	
CVE識別番号	

5.付録

5.1 危険度判定基準

静的な重大度と動的な脆弱性優先度評価（VPR）を使用して、脆弱性をどれだけ緊急に修正する必要があるかを定量化します。静的な重大度の指標として、一般的にCVSSが使用されることが多いのですが、CVSSでは、高～重大に判定される脆弱性が比較的多いため、優先度を決めて対応することが困難だとの見解が一般的です。

本報告書では、以下のような脅威インテリジェンス情報を反映させた指標であるVPRを使用しています。技術的な脅威に加えて、攻撃のトレンドや攻撃の難易度を把握することで、より的確な危険度の判定が可能となります。

脅威インテリジェンスのイベント

- 脆弱性の悪用
- 公開リポジトリへの脆弱性エクスプロイトコードの投稿
- 主流メディアの脆弱性に関する議論
- 脆弱性に関するセキュリティ調査
- ソーシャルメディアチャネルの脆弱性に関する議論
- ダークウェブとアンダーグラウンドの脆弱性に関する議論
- ハッカーフォーラムの脆弱性に関する議論

VPRスコア範囲による分類基準

危険度	VPRスコアの範囲
重大	9.0～10.0
高	7.0～8.9
中	4.0～6.9
低	0.1～3.9
情報	0または値なし

5.2 評価基準

本報告書における総合評価は、以下に規定される絶対評価によるものです。絶対評価は、A、B、C、D のいずれかのアルファベット1文字で表記され、検査結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

評価レベル	評価基準	検出件数
A	早急に対策が必要な脆弱性は検出されませんでした。	検出件数0件
B	直接的に被害を受ける可能性は低いと推測されますが、脆弱性が確認されております。検出内容を確認の上、対策の検討を行うことを推奨します。	危険度高以上の脆弱性は1件も検出されていないが、危険度中以下の脆弱性検出件数は1件以上
C	被害を受ける可能性のある脆弱性が確認されております。早急に対策の検討を行うことを推奨します。	危険度重大以上の脆弱性は1件も検出されず、危険度高の脆弱性が1件以上検出
D	大きな被害を受けることが懸念される危険性の高い脆弱性が確認されております。早急に対策を行うことを推奨します。	危険度重大の脆弱性が1件以上検出

5.3 免責事項

危険度判定基準は、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ございますので、あらかじめご了承ください。

評価基準は本検査において検出された脆弱性の検出件数を基に、検査結果を簡潔に表現するために作成された独自基準になります。上記評価基準による評価は、あくまでも検査結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますので、あらかじめご了承ください。

本報告書の対策を実施する前に、対策の影響度について検討し、対応の可否をご判断ください。弊社では、設定変更後のトラブルについて、責任を負いかねます。また、本報告書の対策によって、全てのセキュリティ対策を網羅できるものではない事についてご了承下さい。

具体的な対策方法については販売代理店様、メーカー様に別途お問合せください。

また、弊社は検査結果により生成された情報及び本報告書に記載された事項に関して、是正処置等の責任を負わないものとします。

その他、以下URLから参照可能なサービス利用規約に準じます。

https://www.singleid.jp/wp-content/uploads/2021/09/SingleID_UserAgreement.pdf

5.4 お問い合わせ

本報告書に関するご質問は、報告書のご提出日より起算して１か月承ります。

また、本レポートを基に対策を実施される場合に、個別の実施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下さい。

お問合せ先　https://www.singleid.jp/contact/