الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1524

(2012/03)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل مواطن الضعف/الحالة

تعديد مواطن الضعف الشائعة (CWE)

التوصيـــة ITU-T X.1524

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	**X.1539–X.1520**
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T X.1524

تعديد مَواطن الضعف الشائعة (CWE)

ملخص

تقدم التوصية ITU-T X.1524 الخاصة باستعمال عملية تعديد مواطن الضعف الشائعة (CWE) وسيلة بنّاءة لتبادل مواطن الضعف في أمن المعلومات بحيث تقدم أسماء مشتركة للمشكلات المعروفة للجمهور في برمجيات تجارية أو مفتوحة المصدر تستعمل في شبكات الاتصالات أو في أجهزة المستعملين النهائيين أو في أي أنماط أخرى من تكنولوجيا المعلومات والاتصالات القادرة على تشغيل برمجيات. والهدف من تعديد مواطن الضعف الشائعة هو إتاحة مزيد من الفعالية في مناقشة ووصف واختيار واستعمال أدوات وخدمات أمن البرمجيات التي يمكنها اكتشاف مواطن الضعف هذه في شفرة المصدر وأنظمة التشغيل فضلاً عن تحسين فهم وإدارة مواطن ضعف البرمجيات المتعلقة بالمعمارية والتصميم. وتعرّف هذه التوصية استعمال عملية تعديد مواطن الضعف المشتركة هذه بحيث توفر آلية من أجل أدوات وخدمات وقواعد معارف أمن البرمجيات وقدرات أخرى يتعين استعمالها معاً ولتسهيل المقارنة فيما بين أدوات وخدمات الأمن. وتوفر عملية CWE كذلك معلومات داعمة في السياق عن المخاطر والآثار المحتملة ومعلومات الإعداد ومعلومات تقنية مفصلة عن ما الذي تعنيه مواطن ضعف البرمجيات بالنسبة لنظام برمجيات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1524	2012-03-02	17

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

تصف التوصية المتعلقة بتعديد مواطن الضعف الشائعة (CWE) طريقة استعمال عملية CWE التي هي عبارة عن وسيلة بناءة لتبادل مجموعة موحدة وقابلة للقياس من مواطن الضعف التي تشوب البرمجيات بهدف تقديم أسماء موحدة للمشكلات المعروفة للجمهور. والهدف من عملية تعديد مواطن الضعف الشائعة هو تسهيل إتاحة مزيد من الفعالية في مناقشة أدوات وخدمات أمن البرمجيات ووصفها واختيارها واستعمال هذه الأدوات والخدمات القادرة على اكتشاف مواطن الضعف هذه في شفرة المصدر وأنظمة التشغيل فضلاً عن تحسين فهم وإدارة مواطن ضعف البرمجيات المتعلقة بالمعمارية والتصميم.

والمُزمع من عملية CWE هو أن تكون شاملة فيما يخص معرفة الأسباب التي تقف وراء مواطن الضعف والتعرض المعروفة جيداً للعامة، سواء كانت متأتية من مواطن ضعف تشوب معمارية البرمجيات أم تصميمها أم تشفيرها أم توزيعها. ومع أن عملية CWE تُصمّم بحيث تتضمن معلومات وافية، فإن تركيزها الأساسي ينصبّ على تحديد مواطن الضعف التي يمكن أن تسبب مواضع الهشاشة والتعرض. وسلطة المراجعة هي التي تحدد المطابقة بشأن استعمال معرّفات عملية CWE على النحو المحدد في هذه التوصية.

وتعزز عملية CWE الأعمال القائمة حالياً داخل الأوساط المعنية بالأمن السيبراني، من قبيل العدد الكبير لمختلف نقاط الضعف التي حددتها في العالم الحقيقي التوصية ITU-T X.1520 – مواطن الضعف والتعرض الشائعة (CVE). ويُستفاد من مصادر ونماذج كثيرة لوضع التعاريف المحددة والموجزة للعناصر الخاصة بقائمة تعديد مواطن الضعف الشائعة وبيان هياكل شجرة التصنيف. وبالإضافة إلى ذلك، تُجرى عمليات تقابل مناسبة بين أسماء مواطن الضعف الشائعة (CWE) وأسماء مواطن الضعف والتعرض الشائعة (CVE) بحيث يكون لكل معرّف هوية مواطن الضعف الشائعة قائمة بأسماء CVE المحددة تنتمي إلى فئة CWE من فئات مواطن الضعف التي تشوب أمن البرمجيات. وعند إعداد قائمة CWE وشجرة التصنيف، يُراعى تحقيق أقصى قدر من التغطية الشاملة لجميع المجالات النظرية والتجارية والتقنية المناسبة.

وتكافئ هذه التوصية وتتوافق من الناحية التقنية مع "المتطلبات والتوصية المعنية بتوافق وفعالية مواطن الضعف الشائعة"، الإصدار 1.0 (version 1.0)، المؤرخة 28 يوليو 2011، والتي يمكن الاطلاع عليها على الموقع التالي: [https://cwe.mitre.org/compatible/requirements_v1.0.html].

تعديد مواطن الضعف الشائعة (CWE)

1 مجال التطبيق

تقدم هذه التوصية الخاصة باستعمال عملية تعديد مواطن الضعف الشائعة (CWE) "وسيلة بناءة" لتبادل المعلومات عالمياً عن مواطن الضعف التي تشوب أمن أنظمة البرمجيات فيما يخص معمارية هذه الأنظمة، أو تصميمها، أو شفرتها، أو توزيعها، والتي يمكن أن تحولها إلى أنظمة غير آمنة وغير موثوقة ومعرضة لخطر الهجمات. وبمقدور الأدوات الأمنية، وخدمات التقييم، وبعض أنواع المراجعات الأمنية أن تكشف عن هذه الأنماط من مواطن ضعف البرمجيات. وغالباً ما يُشار إلى هذه "الوسيلة البناءة" باسم "توافق تعديد مواطن الضعف الشائعة (CWE)"، وهي تحدد الاستعمال السليم لعملية تعديد CWE. وموطن الضعف الذي يشوب أمن المعلومات هو عبارة عن خطأ في البرنامج قد يتسبب في نقطة ضعف يمكن أن يستغلها قراصنة الحاسوب للتمكن من النفاذ إلى نظام أو شبكة ما. ولا تندرج عملية تخصيص معرفات هوية مواطن الضعف الشائعة (CWE) ضمن نطاق هذه التوصية. ويرد في التذييل 1 قائمة بوسائل تخزين معرفات هوية مواطن الضعف الشائعة ومعلومات السياق المرتبطة بها.

والمُزمع من عملية CWE الوارد تعريف استعمالها في هذه التوصية هو أن تكون شاملة بالنسبة لمعمارية البرمجيات وتصميمها وتشفيرها وأخطاء الاستعمال التي تكون في العادة الأسباب الأساسية لمواطن الضعف والتعرض. ففي حين أن عملية CWE مصممة بحيث تتضمن معلومات مكتملة، ينصبّ التركيز الأساسي على التعريف والتثقيف والوصف لهذه المسببات الأساسية لمواطن الضعف والتعرض بحيث يمكن تفاديها من جانب مطوري البرمجيات وإجراء الاختبارات بشأن وجودها من عدمه وإدارتها من جانب أفرقة التطوير فضلاً عن الإبلاغ عنها بصورة متسقة من جانب أدوات وخدمات الأمن.

وتكافئ هذه التوصية وتتوافق من الناحية التقنية مع "المتطلبات والتوصية المعنية بتوافق وفعالية مواطن الضعف الشائعة"، الإصدار 1.0 (version 1.0)، المؤرخة 28 يوليو 2011، والتي يمكن الاطلاع عليها على الموقع التالي: [https://cwe.mitre.org/compatible/requirements_v1.0.html].

2 المراجع

لا يوجد.

3 التعاريف

1.3 المصطلحات المعرّفة في توصيات أخرى

لا يوجد.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 النسبة المئوية للدقة (accuracy percentage): النسبة المئوية للعناصر الأمنية في عيّنة المراجعة التي تشير إلى المعرفات الصحيحة لهوية مواطن الضعف الشائعة.

2.2.3 القدرة (capability): هي عبارة عن أداة تقييم، أو بيئة تنمية متكاملة، أو أداة لمراجعة الشفرات، أو أداة للتحقق من الشفرات، أو قاعدة بيانات، أو موقع على الويب، أو نشرة، أو خدمة تقدم معلومات عن التنفيذ، أو التصميم، أو مواطن الضعف على مستوى المعمارية التي من شأنها أن تسبب موطن ضعف يمكن استغلاله في أمن البرمجيات.

3.2.3 استمارة تقييم متطلبات التوافق إزاء مواطن الضعف الشائعة: تحتوي استمارة التقييم هذه على مجموعة أسئلة تطلب من مالك القدرة توثيق مطابقته مع شروط التوافق الواردة في هذه التوصية بالمراجع النصية أو الصورية أو مراجع الويب، وعلى تعليمات تتعلق بمكان ملء الاستمارة وتقديمها أو بطلب توضيحات من سلطة المراجعة حول طريقة ملء استمارة التقييم.

4.2.3 استمارة تقييم متطلبات الفعالية إزاء مواطن الضعف الشائعة: تحتوي استمارة التقييم هذه على مجموعة أسئلة تطلب من مالك القدرة توثيق مطابقته مع شروط الفعالية الواردة في هذه التوصية بالمراجع النصية أو الصورية أو مراجع الويب، وعلى تعليمات تتعلق بمكان ملء الاستمارة وتقديمها أو بطلب توضيحات من سلطة المراجعة حول طريقة ملء استمارة التقييم.

5.2.3 اختبار الفعالية (effectiveness testing): عملية تحديد ما إذا كانت القدرة فعالة في تعديد مواطن الضعف الشائعة (CWE).

6.2.3 المقارنة/التقابل (map/mapping): تحديد العلاقات بين عناصر موطن الضعف في وسيلة تخزين وبنود مواطن الضعف الشائعة المرتبطة بهذه العناصر.

7.2.3 المالك (owner): هو وصي يتولى مسؤولية القدرة (سواء كان شخصاً حقيقياً أم شركة فعلية).

8.2.3 وسيلة التخزين (repository): مجموعة صريحة أو ضمنية من العناصر المتعلقة بمواطن الضعف الأمنية المتصلة بالبرمجيات، تدعم قدرة ما، مثل قاعدة بيانات خاصة بمواطن الضعف الأمنية أو مجموعة مخططات في محلّل للشفرات، أو موقع على الويب.

9.2.3 المراجعة (review): عملية تحديد توافق قدرة ما مع مواطن الضعف الشائعة أو عدم توافقها معها.

10.2.3 سلطة المراجعة (review authority): كيان يقوم بالمراجعة أو اختبار الفعالية ويُخوّل بسلطة منح صفة متوافق مع مواطن الضعف الشائعة أو فعال إزاء هذه المواطن.

تجدر الإشارة إلى أن التذييل II يحتوي على قائمة بسلطات المراجعة.

11.2.3 إصدار المراجعة (review version): الإصدار المؤرخ من مواطن الضعف الشائعة الذي يُستعمل للبتّ في مدى توافق قدرة ما مع مواطن الضعف الشائعة أو فعاليتها إزاء هذه المواطن.

12.2.3 العنصر الأمني (security element): سجل في قاعدة بيانات أو مسبار تقييم أو توقيع أو أي عنصر آخر مرتبط بموطن ضعف محدد.

13.2.3 المهمة (task): أداة سبر أو تفحّص أو توقيع أو عنصر آخر يؤدي عملاً معيناً يُحصل منه على معلومات أمنية (أي العناصر الأمنية).

14.2.3 نتائج الاختبار (test results): بيانات تمثل نتائج اختبار مدى الفعالية.

15.2.3 الأداة (tool): تطبيق برمجيات أو جهاز يفحص جزءاً من البرمجيات، أو أداة ثنائية، أو أي أداة أخرى مصنوعة يدوياً، ويعطي معلومات عن مواطن الضعف الأمنية، من قبيل محلّل أمن شفرات المصدر أو أداة لتقييم جودة الشفرات أو أداة التحقق من الشفرات أو بيئة تطوير.

16.2.3 المستعمل (user): مستهلك للقدرة أو مستهلك محتمل لها.

17.2.3 نقطة التعرض (vulnerability): أي موطن ضعف في البرمجيات يمكن استغلاله لانتهاك حرمة نظام ما أو المعلومات التي يحتويها (بناء على التوصية b-ITU-T X.1500).

18.2.3 موطن الضعف: هو قصور أو عيب في شفرة البرنامج، أو تصميمها، أو معماريتها، أو نشرها، قد يصبح في مرحلة ما نقطة تعرض، أو قد يسهم في إدخال نقاط تعرض أخرى.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

ASCII النظام الأمريكي الموحّد لتبادل المعلومات (*American Standard Code for Information Interchange*)

CCR تمثيل الادعاء بالتغطية (*Coverage Claim Representation*)

CGI السطح البيني لبوابة مشتركة (*Common Gateway Interface*)

CWE تعديد مواطن الضعف الشائعة (*Common Weakness Enumeration*)

GUI السطح البيني البياني للمستعمل (*Graphical User Interface*)

HTML لغة وسم النصوص الفائقة (*HyperText Markup Language*)

HTTP بروتوكول نقل النص الفائق (*HyperText Transfer Protocol*)

ICT تكنولوجيا المعلومات والاتصالات (*Information and Communications Technology*)

PDF نسق الوثائق المحمولة (*Portable Document Format*)

POC جهة الاتصال (*Point of Contact*)

URL موقع الموارد الموحد (*Uniform Resource Locator*)

XML لغة وسم قابلة للتوسيع (*Extensible Markup Language*)

5 الاصطلاحات

لا يوجد.

6 المتطلبات رفيعة المستوى

تعرّف البنود الواردة أدناه المفاهيم والأدوار والمسؤوليات المتصلة باستعمال معرفات هوية تعديد مواطن الضعف الشائعة (CWE) على الوجه الأمثل لأغراض تبادل البيانات عبر جميع القدرات المستقلة لمواطن الضعف الأمنية (من أدوات ووسائل تخزين وخدمات) للتمكين من استعمال قدرات مواطن الضعف الأمنية هذه مجتمعة معاً، وتسهيل إجراء مقارنة بين أدوات وخدمات مواطن الضعف الأمنية.

1.6 يجب أن يكون مالك القدرة كياناً قانونياً سارياً، أي منظمة ما أو شخصاً محدداً، وأن يكون في حوزته رقم هاتف صالح وعنوان بريدي إلكتروني وعنوان بريدي عادي.

2.6 يجب أن تقدم القدرة قيمة أو معلومات إضافية تتعدى تلك المقدمة في مواطن الضعف الشائعة نفسها (أي الاسم والوصف والمخاطر والمراجع وما يتصل بها من معلومات عن مواطن الضعف).

3.6 يجب أن يزوِّد مالك القدرة سلطة المراجعة بنقطة اتصال تقنية مؤهلة للإجابة على الأسئلة المتصلة بمدى دقة التقابل وأية وظيفة للقدرة متصلة بمواطن الضعف الشائعة، ولتنسيق اختبار القدرة دعماً لتقييم مدى فاعليتها في تحديد هوية مواطن الضعف الشائعة.

4.6 يجب أن تكون القدرة متاحة للجمهور، أو لمجموعة من المستهلكين، في شكل منتج أو إصدار عام، كأن تكون متيسرة على موقع ويب عام، أو مقدمة للاستعمال كمصدر مفتوح، أو يمكن اقتناؤها أو كخدمة تتاح بناء على عقد.

5.6 فيما يخص مدى التوافق مع مواطن الضعف الشائعة، يجب أن يزوّد مالك القدرة سلطة المراجعة بنسخة مكتملة من "استمارة تقييم متطلبات التوافق إزاء مواطن الضعف الشائعة".

6.6 يجب أن يزوّد مالك القدرة سلطة المراجعة بسبيل نفاذ حر إلى وسيلة التخزين كيما يتسنى للسلطة تحديد ما إذا كانت هذه الوسيلة تفي بجميع الشروط المتصلة بالتحقق من مدى دقة التقابل.

7.6 يجب أن يسمح مالك القدرة لسلطة المراجعة باستخدام هذه الوسيلة لتحديد أي مواطن ضعف ينبغي إضافتها إلى قائمة مواطن الضعف الشائعة.

8.6 يجب أن تكون القدرة متوافقة مع مواطن الضعف الشائعة تحقيقاً لفعالية هذه المواطن.

9.6 تحقيقاً لفعالية مواطن الضعف الشائعة، يجب أن يزوّد مالك القدرة سلطة المراجعة بنسخة مكتملة من "استمارة تقييم شروط فعالية مواطن الضعف الشائعة".

10.6 تحقيقاً لفعالية مواطن الضعف الشائعة، يجب أن يزوّد مالك القدرة سلطة المراجعة بنتائج اختبار مدى الفعالية كيما يتسنى للسلطة أن تبت فيما إذا كانت هذه القدرة تستوفي جميع الشروط المتصلة بالتحقق من مدى الفعالية.

11.6 يجب أن يوافق مالك القدرة على أن يتقيّد بجميع الشروط الإلزامية المتعلقة بالتحقق من توافق مواطن الضعف الشائعة وفعاليتها، والتي تشمل الشروط الإلزامية المتعلقة بالنوع المحدد من القدرة.

12.6 فيما يخص التوافق مع مواطن الضعف الشائعة، يجب أن تسمح القدرة للمستعملين بتحديد أماكن العناصر الأمنية التي تستخدم معرفات هوية مواطن الضعف الشائعة ("مواطن الضعف الشائعة القابلة للبحث").

13.6 عندما تقدم القدرة عناصر أمنية للمستعمل في إطار تحقيق التوافق مع مواطن الضعف الشائعة، يجب أن تسمح للمستعمل بالحصول على معرفات هوية مواطن الضعف الشائعة ذات الصلة ("نواتج مواطن الضعف الشائعة").

14.6 بالنسبة للتوافق مع مواطن الضعف الشائعة، يجب أن يربط تقابل القدرة ربطاً دقيقاً العناصر الأمنية بمعرفات الهوية المناسبة لمواطن الضعف الشائعة ("دقة التقابل").

15.6 فيما يتعلق بالتوافق مع مواطن الضعف الشائعة، يجب أن تصف الوثائق المتعلقة بالقدرة وصفاً كافياً مواطن الضعف الشائعة وتوافقها وطريقة استعمال الوظيفة المتصلة بها في القدرة ("وثائق مواطن الضعف الشائعة").

16.6 بالنسبة للتوافق مع مواطن الضعف الشائعة، يجب أن تبيّن وثائق القدرة المتاحة للجمهور بشكل صريح قائمة بأسماء معرفات هوية مواطن الضعف الشائعة التي يرى مالك القدرة أنها القدرة اللازمة لتغطية جزء من وظيفتها ("تغطية مواطن الضعف الشائعة").

17.6 فيما يخص التوافق مع مواطن الضعف الشائعة، ينبغي لموقع الويب الخاص بالقدرة المتاح للجمهور أن يؤمّن صراحة تغطية قدرة مواطن الضعف الشائعة بوصفها وثيقة (وثائق) بالنسق XML تمثل الادعاء بتغطية المواطن المذكورة (CCR).

18.6 فيما يتعلق بفعالية مواطن الضعف الشائعة، يجب أن تُنشر على موقع الويب لهذه المواطن نتائج تقييم قدرة مجموعات الاختبارات المحددة لمعرفات هوية مواطن الضعف الشائعة (المبينة بوصفها تغطية قدرة مواطن الضعف الشائعة) ("نتائج اختبار مواطن الضعف الشائعة").

19.6 يجب أن تبين القدرة الإصدار المؤرَّخ المستعمل من مواطن الضعف الشائعة ("الإصدار المستعمل").

20.6 يجب أن تفي القدرة بأية شروط إضافية خاصة بهذا النوع من القدرة تحديداً، على النحو المبيّن في الملحق A.

21.6 يجب أن تفي القدرة بجميع شروط وسائط توزيعها، على النحو المحدد في الملحق B.

22.6 ولا يلزم أن تقوم القدرة بأي من الأمرين التاليين:

- استعمال الأوصاف أو المراجع نفسها التي تستعملها مواطن الضعف الشائعة؛
- إدراج اسم كل موطن من مواطن الضعف الشائعة في وسيلة التخزين الخاصة بها.

23.6 إذا لم تستوف القدرة جميع الشروط المعمول بها أعلاه (الفقرات من 1.6 وحتى 22.6)، فيجب ألا يعلن المالك حينها عن أنها متوافقة أو فعالة إزاء مواطن الضعف الشائعة.

7 الدقة

لا يسهّل توافق مواطن الضعف الشائعة من عملية تبادل البيانات والترابط إلا إذا كان تقابل القدرة دقيقاً. ولهذا، يجب أن تفي القدرات المتوافقة من حيث مواطن الضعف الشائعة بالحد الأدنى من شروط الدقة الواردة أدناه.

1.7 يجب أن تبلغ نسبة دقة وسيلة التخزين 100%.

2.7 خلال فترة المراجعة، يجب أن يصحح مالك القدرة أية أخطاء في التقابل تكتشفها سلطة المراجعة.

3.7 بعد فترة المراجعة، ينبغي أن يصحح مالك القدرة أي خطأ في التقابل في غضون إطار زمني معقول بعد التاريخ الذي أُبلغ فيه أول مرة عن الخطأ، أي في غضون إصدارين اثنين (2) من إصدارات وسيلة التخزين أو ستة (6) أشهر، أيهما أقصر.

4.7 ينبغي لمالك القدرة أن يُعد ويوقع بياناً يفيد فيه، وفقاً لأفضل ما هو متوافر لديه من معلومات، بعدم وجود أخطاء في التقابل.

5.7 إذا كانت القدرة تستند إلى قدرة أخرى متوافقة من حيث مواطن الضعف الشائعة أو تستعملها (القدرة "المصدر")، وأصبح مالكها مدركاً لأخطاء التقابل في القدرة المصدر، يجب أن يرفع المالك تقريراً بشأن هذه الأخطاء إلى مالك القدرة المصدر.

8 الفعالية

تركز الفعالية على تزويد المستعملين المحتملين برؤية تبين إمكانات القدرة على تشخيص مواطن الضعف المقابلة في البرمجيات. ويكتسي أمر التبصر في إمكانية القدرة على إيجاد مواطن الضعف إزاء مختلف مستويات التعقيد أهمية بالنسبة للمستعملين عند النظر في استعمال إحدى القدرات أو التعويل على نتائج مستعمل آخر للقدرة. لذا يجب أن تفي قدرات الفعالية حيال مواطن الضعف الشائعة بشروط الحد الأدنى للفعالية الواردة أدناه.

1.8 عند استعمال الجزء المناسب من "استمارة تقييم الشروط المتعلقة بفعالية مواطن الضعف الشائعة"، على مالك القدرة أن يعلن عن معرفات هوية مواطن الضعف الشائعة التي يزعم أنها فعالة في تحديد المواقع. ويمكن تحقيق ذلك باستعمال وثيقة (وثائق) بالنسق XML تمثل الادعاء بتغطية (CCR) مواطن الضعف الشائعة.

2.8 وبالنسبة لمعرفات هوية مواطن الضعف الشائعة المعلن عنها، على مالك القدرة أن يطلب مجموعات الاختبار المناسبة كيما يتسنى له أن يستعمل القدرة لتقييم هذه المجموعات إزاء جميع مواطن الضعف المقابلة لمعرفات هوية مواطن الضعف الشائعة المعلن عنها.

3.8 على مالك القدرة أن يقدم في غضون إطار زمني متفق عليه النتائج التي يحصل عليها من تقييم مجموعات اختبار قدرته.

4.8 تورد النتائج قائمة باسم كل ملف من ملفات مجموعات الاختبار التي جرى تقييمها، ورقم سطر كل واحد من مواطن الضعف المحددة الموقع جنباً إلى جنب مع معرفات الهوية المناسبة لمواطن الضعف الشائعة.

5.8 على مالك القدرة أن يُعد ويوقع بياناً يوافق فيه على أن تُنشر نتائج اختبار قدرته على موقع الويب الخاص بمواطن الضعف الشائعة.

6.8 على مالك القدرة أن يقدم "استمارة منقحة لتقييم الشروط المتعلقة بفعالية مواطن الضعف الشائعة" مرفقة بقائمة محدثة بأسماء معرفات هوية مواطن الضعف المذكورة التي يزعم أنها فعالة في تحديد المواقع من أجل إعادة تطبيق اختبارات الفعالية على مجموعة مختلفة من معرفات هوية مواطن الضعف الشائعة. ويمكن تحقيق ذلك باستعمال وثيقة (وثائق) محدثة بالنسق XML تمثل الادعاء بتغطية (CCR) مواطن الضعف الشائعة.

9 الوثائق

تنطبق الشروط التالية على الوثائق التي تُقدَّم مع القدرة.

1.9 يجب أن تتضمن الوثائق وصفاً موجزاً لمواطن الضعف الشائعة ومدى توافق هذه المواطن، حيث يمكن أن يستند إلى أجزاء حرفية من الوثائق المحملة من على موقع الويب الخاص بمواطن الضعف الشائعة.

2.9 يجب أن تصف الوثائق الطريقة التي يمكن أن يجد بها المستعمل عناصر أمنية فردية في وسيلة التخزين الخاصة بالقدرة عن طريق استعمال معرفات هوية مواطن الضعف الشائعة.

3.9 يجب أن تصف الوثائق الطريقة التي يمكن أن يحصل بها المستعمل على معرفات هوية مواطن الضعف الشائعة انطلاقاً من عناصر فردية في وسيلة التخزين الخاصة بالقدرة.

4.9 إذا كانت الوثائق تتضمن فهرساً، فينبغي أن تشمل إحالات إلى الوثائق المتصلة بمواطن الضعف الشائعة تحت مصطلح "مواطن الضعف الشائعة".

10 استعمال إصدار مواطن الضعف الشائعة

يجب أن يعرف المستعملون رقم إصدار مواطن الضعف الشائعة المستعمل في وسيلة التخزين الخاصة بقدرة ما فيما يتعلق بتقابلها مع مواطن الضعف الشائعة. وبإمكان مالك القدرة أن يبيّن سريان التقابل من خلال استعمال رقم إصدار مواطن الضعف الشائعة أو تاريخ تحديث التقابل.

1.10 يجب أن تحدد القدرة رقم إصدار مواطن الضعف الشائعة أو تاريخ تحديثه الذي استُخدم في إجراء التقابل أو تحديثه من خلال واحد على الأقل من الأمور التالية: تغيير السجلات أو قوائم السمات الجديدة أو ملفات المساعدة أو غيرها من الآليات المحددة. وتكون القدرة "محدَّثة" بالنسبة لذلك الإصدار أو تاريخ التحديث.

2.10 ينبغي تحديث كل إصدار جديد للقدرة بالنسبة لأحد إصدارات مواطن الضعف الشائعة الذي لم يمر على نشره أكثر من أربعة (4) أشهر قبل إتاحة القدرة لمستعمليها. وإذا لم تستوف قدرة ما هذا الشرط، فإنها تكون "متقادمة".

3.10 ينبغي لمالك القدرة أن يعلن عن السرعة التي سيحدِّث بها وسيلة التخزين الخاصة بالقدرة بعد ظهور إصدار جديد لمواطن الضعف الشائعة أو تحديث للإصدار المستعمل على موقع الويب الخاص بمواطن الضعف الشائعة.

11 إلغاء توافق مواطن الضعف الشائعة

فيما يلي وصف لمسؤوليات سلطة المراجعة بالنسبة لإلغاء توافق مواطن الضعف الشائعة.

1.11 إذا تحققت سلطة مراجعة من توافق قدرة ما أو فعاليتها إزاء مواطن الضعف الشائعة، لكن ظهرت أدلة بينت لسلطة المراجعة في وقت لاحق عدم الاستمرار في الوفاء بالشروط، يجوز لهذه السلطة حينئذ أن تلغي تصديقها.

1.1.11 يجب أن تحدد سلطة المراجعة الشروط المحددة التي لا يجري الوفاء بها.

2.11 يجب أن تحدد السلطة ما إذا كانت إجراءات أو ادعاءات مالك القدرة "مضلِّلة عن قصد".

1.2.11 يجوز لسلطة المراجعة أن تفسر جملة "مضلِّلة عن قصد" على النحو الذي تريده.

3.11 ينبغي ألا تنظر سلطة المراجعة في إلغاء التوافق بالنسبة لمواطن الضعف الشائعة لقدرة معينة أكثر من مرة واحدة في كل ستة (6) أشهر.

4.11 يجب أن توجه سلطة المراجعة إلى مالك القدرة أو جهة الاتصال التقنية إنذاراً بالإلغاء قبل الوقت المُزمع إجراء الإلغاء فيه بشهرين (2) على الأقل.

1.4.11 إذا اكتشفت سلطة المراجعة أن إجراءات أو ادعاءات مالك القدرة مضللة عن قصد، يجوز لهذه السلطة عدم التقيد بفترة الإنذار.

5.11 إذا كان المالك يرى أن الشروط مستوفاة، فيجوز له أن يرد على إنذار الإلغاء بتقديم تفاصيل محددة تبين الأسباب التي تقف وراء استيفاء القدرة للشروط المعنية.

6.11 إذا عدل المالك القدرة بحيث تتقيد بالشروط المعنية خلال فترة الإنذار، فينبغي لسلطة المراجعة إنهاء إجراء الإلغاء بالنسبة للقدرة.

7.11 يجوز لسلطة المراجعة أن تؤجل تاريخ الإلغاء.

8.11 يجب أن تعلن سلطة المراجعة عن إلغاء التوافق أو الفعالية إزاء مواطن الضعف الشائعة بالنسبة للقدرة على موقع الويب لهذه المواطن.

9.11 إذا وجدت سلطة المراجعة أن إجراءات المالك فيما يتعلق بشروط التوافق أو الفعالية إزاء مواطن الضعف الشائعة مضللة بشكل مقصود، يستمر الإلغاء لسنة واحدة على الأقل.

10.11 يجوز لسلطة المراجعة إعلان سبب الإلغاء.

11.11 يجوز لمالك القدرة أن ينشر على الموقع نفسه إعلاناً للجمهور بشأن الإلغاء.

12.11 إذا أُلغي التصديق، لا يجوز للمالك التقدم بطلب لإجراء مراجعة جديدة خلال فترة الإلغاء.

12 سلطة المراجعة

1.12 يجب أن تراجع سلطة المراجعة القدرة لتحديد مدى توافقها وفعاليتها إزاء مواطن الضعف الشائعة بالنسبة لإصدار معين من مواطن الضعف الشائعة، أي إصدار المراجعة.

2.12 يجب أن تحدد سلطة المراجعة بشكل واضح إصدار المراجعة الذي استُعمل من أجل تحديد توافق القدرة أو فعاليتها.

3.12 يجب أن تحدد سلطة المراجعة بشكل واضح رقم إصدار وثيقة شروط التوافق والفعالية من حيث مواطن الضعف الشائعة، التي استُخدمت من أجل تحديد توافق القدرة أو فعاليتها.

4.12 على سلطة المراجعة أن تراجع كل عنصر في وسيلة تخزين القدرة لأغراض التحقق من دقة تقابل مواطن الضعف الشائعة.

5.12 ينبغي لسلطة المراجعة أن تراجع مدى دقة تقابل القدرة مرة واحدة على الأقل سنوياً.

الملحق A

الشروط الخاصة بالنوع

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

نظراً لأن مجموعة واسعة من القدرات تستخدم مواطن الضعف الشائعة، فقد تكون لدى أنواع معينة من القدرات سمات فريدة تستدعي اهتماماً خاصاً فيما يتعلق بالتوافق من حيث مواطن الضعف الشائعة.

1.A يجب أن تستوفي القدرة جميع الشروط الإضافية التي تتصل بنوع معين من أنواع القدرات.

1.1.A إذا كانت القدرة أداة لتقييم مواطن الضعف الشائعة، أو محللاً أمنياً لشفرة المصدر أو شفرة اثنينية أو أداة لتقييم نوعية الشفرة أو وسيلة للتحقق من الشفرة أو بيئة تطوير أو منتجاً يجمع نتائج نوع واحد أو أكثر من أنواع هذه البنود، يجب أن تستوفي القدرة شروط الأداة، الفقرات من 1.2.A إلى 8.2.A.

2.1.A إذا كانت القدرة خدمة (مثل خدمة تقييم النواحي الأمنية، أو خدمة تثقيف أو تدريب، أو خدمة لمراجعة الشفرات والتصاميم)، فيجب أن تستوفي شروط الخدمة الأمنية، الفقرات من 1.3.A إلى 5.3.A.

3.1.A إذا كانت القدرة قاعدة بيانات على الخط للمسائل الأمنية أو مواطن الضعف في برمجيات التطبيق، أو مورداً قائماً على شبكة الويب، أو موقعاً لاستقاء المعلومات، فيجب أن تستوفي شروط القدرة على الخط، الفقرات من 1.4.A إلى 3.4.A.

2.A شروط الأداة

فيما يلي الشروط الخاصة بالأداة.

1.2.A يجب أن تسمح الأداة للمستعمل باستخدام معرفات هوية مواطن الضعف الشائعة لتحديد مواقع المهام ذات الصلة في تلك الأداة ("مواطن الضعف الشائعة القابلة للبحث") من خلال توفير واحد على الأقل من الأمور التالية: وظيفة إيجاد "Find" أو بحث "Search" أو تقابل بين أسماء مهام تلك الأداة ومعرفات هوية مواطن الضعف الشائعة الخاصة بها أو آلية أخرى ترى سلطة المراجعة أنها تفي بالغرض.

2.2.A بالنسبة لأي تقرير يعرِّف عناصر أمنية فردية، يجب أن تسمح الأداة للمستعمل بتحديد معرفات هوية مواطن الضعف الشائعة ذات الصلة بهذه العناصر ("نواتج مواطن الضعف الشائعة") من خلال القيام بواحد على الأقل من الأمور التالية: إدراج معرفات هوية مواطن الضعف الشائعة بشكل مباشر في التقرير أو تقديم تقابل بين أسماء مهام الأداة ومعرفات هوية مواطن الضعف الشائعة أو استعمال آلية أخرى ترى سلطة المراجعة أنها تفي بالغرض.

3.2.A يجب أن تبيّن وثائق القدرة المتاحة للجمهور بشكل صريح قائمة بأسماء معرفات هوية مواطن الضعف الشائعة التي يرى مالك القدرة أن الأداة فعالة في تحديد المواقع داخل البرمجيات ("تغطية الادعاء بالتوافق إزاء مواطن الضعف الشائعة").

4.2.A قد يوفر موقع الويب الخاص بالقدرة المتاح للجمهور تغطية الادعاء بالتوافق إزاء مواطن الضعف الشائعة بوصفها وثيقة (وثائق) بالنسق XML تمثل الادعاء بتغطية المواطن المذكورة (CCR).

5.2.A يجب أن تستوفي أية تقارير أو تقابلات مطلوبة شروط الوسائط على النحو المحدد في الملحق B.

6.2.A ينبغي للأداة أو مالك القدرة تزويد المستعمل بقائمة تضم جميع أسماء معرفات هوية مواطن الضعف الشائعة المقترنة بمهام الأداة.

7.2.A ينبغي للأداة أن تتيح للمستعمل انتقاء مجموعة من المهام من خلال تقديم ملف يتضمن قائمة بأسماء معرفات هوية مواطن الضعف الشائعة.

8.2.A ينبغي للسطح البيني للأداة أن يتيح للمستعمل تصفح مجموعة من المهام وانتقائها وإلغاء انتقائها باستخدام معرفات هوية فردية لمواطن الضعف الشائعة.

9.2.A إذا لم يكن للأداة مهمة تتصل بمعرِّف من معرّفات هوية مواطن الضعف الشائعة يحدده المستعمل على النحو الوارد في شرطي الأداة 5.2.A أو 6.2.A، ينبغي للأداة إفادة المستعمل بأنها لا تستطيع إنجاز المهمة ذات الصلة.

10.2.A يجب أن يضمن مالك القدرة أن (1) نسبة الإيجابيات الكاذبة أقل من 100 في المائة، أي إذا أفادت الأداة بوجود عنصر أمني معين، فإن ذلك يكون صحيحاً على الأقل في بعض الأحيان، وأن (2) نسبة السلبيات الكاذبة أقل من 100 في المائة، أي إذا وُجد خلل متصل بعنصر أمني محدد، فإن الأداة تعلن في بعض الأحيان بوجود هذا الخلل.

3.A شروط الخدمة الأمنية

يمكن للخدمات الأمنية استخدام الأدوات المتوافقة والمتسمة بالفعالية من حيث مواطن الضعف الشائعة في عملها لكن لا يجوز لها أن تمنح العملاء إمكانية النفاذ المباشر إلى هذه الأدوات. وهكذا، قد يكون من الصعب بالنسبة للعملاء تحديد ومقارنة قدرات خدمات مختلفة. وتعالج شروط الخدمة الأمنية هذا القيد المحتمل.

1.3.A يجب أن تكون الخدمة الأمنية قادرة على استعمال معرفات هوية مواطن الضعف الشائعة لإخبار المستعمل بشأن العناصر الأمنية التي اختبرتها الخدمة أو كشفت عنها أو تناولتها ("مواطن الضعف الشائعة القابلة للبحث") من خلال القيام بواحد أو أكثر من الأمور التالية: تزويد المستعمل بقائمة تضم معرفات هوية مواطن الضعف الشائعة وتحديد العناصر التي اختبرتها الخدمة أو كشفت عنها أو تناولتها أو تزويد المستعمل بتقابل بين عناصر الخدمة ومعرفات هوية مواطن الضعف الشائعة أو الرد على قائمة واردة من المستعمل بمعرفات هوية مواطن الضعف الشائعة من خلال تحديد معرفات هوية مواطن الضعف الشائعة التي اختبرتها الخدمة أو كشفت عنها أو تناولتها أو استخدام آلية أخرى.

2.3.A بالنسبة لأي تقرير يعرِّف عناصر أمنية فردية، يجب أن تسمح الخدمة للمستعمل بتحديد معرفات هوية مواطن الضعف والتعرض الشائعة المتصلة بتلك العناصر ("نواتج مواطن الضعف الشائعة") من خلال القيام بواحد أو أكثر من الأمور التالية: السماح للمستعمل بإدراج معرفات هوية مواطن الضعف الشائعة بشكل مباشر في التقرير أو تزويد المستعمل بتقابل بين العناصر الأمنية ومعرفات هوية مواطن الضعف الشائعة أو استعمال آلية أخرى.

3.3.A يجب أن تدرج أي وثيقة متاحة للجمهور بشكل صريح قائمة بمعرفات هوية مواطن الضعف الشائعة التي يرى مالك القدرة أن الخدمة الأمنية تغطيها بفعالية في عروض هذه الخدمة ("تغطية الادعاء بالتوافق إزاء مواطن الضعف الشائعة").

4.3.A يجوز لموقع الويب الخاص بالقدرة والمتاح للجمهور أن يوفر تغطية الادعاء بالتوافق إزاء مواطن الضعف الشائعة في صورة وثائق بالنسق XML تمثل الادعاء بتغطية مواطن الضعف الشائعة.

5.3.A يجب أن تستوفي أية تقارير أو تقابلات مطلوبة تقدمها الخدمة شروط الوسائط على النحو المحدد في الملحق B.

6.3.A إذا كانت الخدمة تسمح للمستعمل بالنفاذ المباشر إلى منتج يعرِّف عناصر أمنية، ينبغي للمنتج هذا أن يكون متوافقاً وفعالاً من حيث مواطن الضعف الشائعة.

7.3.A يجب أن يضمن المالك أن (1) نسبة الإيجابيات الكاذبة أقل من 100 في المائة، أي إذا أفادت أداة بوجود عنصر أمني معين، فإن ذلك يكون صحيحاً على الأقل في بعض الأحيان، وأن (2) نسبة السلبيات الكاذبة أقل من 100 في المائة، أي إذا وقع حدث متصل بعنصر أمني محدد، فإن الخدمة تُخبر في بعض الأحيان بوقوع هذا الحدث.

4.A شروط القدرة على الخط

وفيما يلي المتطلبات الخاصة بالقدرة على الخط:

1.4.A يجب أن تسمح القدرة على الخط للمستعمل بالحصول على العناصر الأمنية ذات الصلة من وسيلة تخزين القدرة الموجودة على الخط ("مواطن الضعف الشائعة القابلة للبحث") من خلال توفير أحد الأمور التالية: وظيفة للبحث تستعيد معرفات هوية مواطن الضعف الشائعة بالنسبة للعناصر ذات الصلة أو تقابُل يربط كل عنصر بمعرف هوية (معرفات هوية) مواطن الضعف الشائعة أو آلية أخرى.

1.1.4.A ينبغي للقدرة على الخط أن توفر "نموذجاً" لموقع الموارد الموحد (URL) يسمح لأي برنامج حاسوبي بأن ينشئ بسهولة رابطاً ينفذ إلى وظيفة البحث على النحو المبين في شروط القدرة على الخط، الفقرة 1.4.A.

أمثلة:

http://www.example.com/cgi-bin/db-search.cgi?cweid=XXX
http://www.example.com/cwe/xxx.html

2.1.4.A إذا كان الموقع متاحاً لنفاذ الجمهور دون الحاجة إلى عملية تسجيل للدخول، ينبغي للبرنامج cgi أن يقبل الأسلوب "GET".

2.4.A وبالنسبة لأي تقرير يعرِّف عناصر أمنية فردية، يجب أن تسمح القدرة على الخط للمستعمل بتحديد معرفات هوية مواطن الضعف الشائعة ذات الصلة بالنسبة لهذه العناصر ("نواتج مواطن الضعف الشائعة") من خلال القيام بواحد على الأقل من الأمور التالية: السماح للمستعمل بإدراج معرفات هوية مواطن الضعف الشائعة بشكل مباشر في التقرير أو تزويد المستعمل بتقابل بين العناصر الأمنية ومعرفات هوية مواطن الضعف الشائعة أو استعمال آلية أخرى.

3.4.A يجب أن تدرج أي وثيقة متاحة للجمهور بشكل صريح قائمة بمعرفات هوية مواطن الضعف الشائعة التي يرى مالك القدرة أن وسيلة تخزين القدرة على الخط تغطيها ("تغطية الادعاء بتوافق مواطن الضعف الشائعة").

4.4.A يجوز لموقع الويب الخاص بالقدرة والمتاح للجمهور أن يوفر تغطية الادعاء بتوافق مواطن الضعف الشائعة في صورة وثيقة (وثائق) بنسق XML تمثل الادعاء بتغطية مواطن الضعف الشائعة.

5.4.A وإذا كانت القدرة على الخط لا تقدم تفاصيل بشأن عناصر أمنية فردية، فيجب أن تقدم تقابلاً يربط كل عنصر بمعرف (معرفات) هوية مواطن الضعف الشائعة.

الملحق B

شروط الوسائط

(يُشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.B يجب أن تستخدم وسائط النشر التي تستخدمها قدرة متوافقة من حيث مواطن الضعف الشائعة نسقاً للوسائط يغطيه هذا الملحق.

2.B يجب أن يستوفي نسق الوسائط الشروط المحددة الخاصة به.

3.B الوثائق الإلكترونية (لغة وسم النصوص الفائقة (HTML) ومعالج النصوص ونسق الوثائق المحمولة (PDF) ونصوص النظام الأمريكي الموحد لتبادل المعلومات (ASCII) وغيرها)

1.3.B يجب أن تكون الوثيقة في نسق متاح على نطاق واسع وله قارئات تدعم وظيفة إيجاد "Find" أو بحث "Search" ("مواطن الضعف الشائعة القابلة للبحث") مثل نصوص ASCII صرفة أو HTML أو PDF.

2.3.B إذا كانت الوثيقة لا تقدم سوى أسماء أو عناوين قصيرة لعناصر فردية، فيجب أن تشمل قائمة بمعرفات هوية مواطن الضعف الشائعة التي تتصل بتلك العناصر ("نواتج مواطن الضعف الشائعة").

3.3.B ينبغي للوثيقة أن تشمل تقابلاً بين العناصر ومعرفات هوية مواطن الضعف الشائعة، يدرج الصفحات المناسبة بالنسبة لكل عنصر.

4.B السطح البيني البياني للمستعمل (GUI)

فيما يلي الشروط الخاصة بالسطح البيني البياني للمستعمل.

1.4.B على السطح البيني البياني للمستعمل أن يزود المستعمل بوظيفة للبحث تسمح له بإدخال معرف من معرفات هوية مواطن الضعف الشائعة واسترداد العناصر ذات الصلة ("مواطن الضعف الشائعة القابلة للبحث").

2.4.B إذا كان السطح البيني البياني للمستعمل يشمل تفاصيل بشأن عنصر فردي، فيجب أن يدرج معرفات هوية مواطن الضعف الشائعة التي تقابل ذلك العنصر ("نواتج مواطن الضعف الشائعة"). وإذا لم يكن الأمر كذلك، فعلى السطح البيني البياني للمستعمل أن يزود المستعمل بتقابل في نسق يستوفي الشرط 1.3.B المتعلق بالوثائق الإلكترونية.

3.4.B ينبغي للسطح البيني البياني للمستعمل أن يسمح للمستعمل بتصدير البيانات المتعلقة بمواطن الضعف الشائعة أو النفاذ إلى هذه البيانات في نسق بديل يستوفي الشرط 1.3.B المتعلق بالوثائق الإلكترونية.

التذييل I

قائمة بوسائل تخزين معرفات مواطن الضعف الشائعة ومعلومات السياق المرتبطة بها

(لا يُشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

شركة MITRE	cwe.mitre.org/data

التذييل II

قائمة بسلطات المراجعة

(لا يُشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1 شركة MITRE، يمكن الاتصال بها على البريد الإلكتروني cwe@mitre.org.

بيبليوغرافيـــا

[b-ITU-T X.1520] التوصية ITU-T X.1500 (2011)، *نظرة عامة على تبادل معلومات الأمن السيبراني*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبِعَت في سويسرا
جنيف، 2012