

X.1520

(2014/01)

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين
الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني - تبادل معلومات مواطن الضعف/الحالة

مواطن الضعف والتعرض الشائعة

التوصية ITU-T X.1520

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات
شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

X.199-X.1	الشبكات العمومية للبيانات
X.299-X.200	التوصيل البيني للأنظمة المفتوحة
X.399-X.300	التشغيل البيني للشبكات
X.499-X.400	أنظمة معالجة الرسائل
X.599-X.500	الدليل
X.699-X.600	التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام
X.799-X.700	إدارة التوصيل البيني للأنظمة المفتوحة (OSI)
X.849-X.800	الأمن
X.899-X.850	تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)
X.999-X.900	المعالجة الموزعة المفتوحة
X.1029-X.1000	أمن المعلومات والشبكات
X.1049-X.1030	الجوانب العامة للأمن
X.1069-X.1050	أمن الشبكة
X.1099-X.1080	إدارة الأمن
X.1109-X.1100	الخصائص البيومترية
X.1119-X.1110	تطبيقات وخدمات آمنة
X.1139-X.1120	أمن البث المتعدد
X.1149-X.1140	أمن الشبكة المحلية
X.1159-X.1150	أمن الخدمات المتنقلة
X.1169-X.1160	أمن الويب
X.1179-X.1170	بروتوكولات الأمن
X.1199-X.1180	الأمن بين جهتين نظيرتين
X.1229-X.1200	أمن معرفات الهوية عبر الشبكات
X.1249-X.1230	أمن التلفزيون القائم على بروتوكول الإنترنت
X.1279-X.1250	أمن الفضاء السيرياني
X.1309-X.1300	الأمن السيرياني
X.1339-X.1310	مكافحة الرسائل الاقتحامية
X.1519-X.1500	إدارة الهوية
X.1539-X.1520	تطبيقات وخدمات آمنة
X.1549-X.1540	اتصالات الطوارئ
X.1559-X.1550	أمن شبكات المحاسيس واسعة الانتشار
X.1569-X.1560	تبادل معلومات الأمن السيرياني
X.1579-X.1570	نظرة عامة عن الأمن السيرياني
X.1589-X.1580	تبادل مواطن الضعف/الحالة
X.1601-X.1600	تبادل الأحداث/الأحداث العارضة/المعلومات الحدية
X.1639-X.1602	تبادل السياسات
X.1659-X.1640	طلب المعلومات الحدية والمعلومات الأخرى
X.1679-X.1660	تعرف الهوية والاكتشاف
X.1699-X.1680	التبادل المضمون
	أمن الحوسبة السحابية
	نظرة عامة على أمن الحوسبة السحابية
	تصميم أمن الحوسبة السحابية
	أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية
	تنفيذ أمن الحوسبة السحابية
	أشكال أخرى لأمن الحوسبة السحابية

مواطن الضعف والتعرض الشائعة

ملخص

تقدم التوصية ITU-T X.1520 التي تخص استعمال مواطن الضعف والتعرض الشائعة (CVE) وسيلة منظمة لتبادل المعلومات الأمنية بشأن مواطن الضعف والتعرض الشائعة، توفر أسماء مشتركة للمشاكل التي يعرفها الجمهور في مجال البرمجيات التجارية أو برمجيات المصدر المفتوح المستعملة في شبكات الاتصالات أو أجهزة المستعمل النهائي أو أي أنواع أخرى من تكنولوجيا المعلومات والاتصالات القادرة على تشغيل برمجيات. والهدف من هذه التوصية هو تعريف استعمال مواطن الضعف والتعرض الشائعة من أجل زيادة تسهيل تبادل البيانات عبر قدرات منفصلة لتحديد مواطن الضعف (أدوات ووسائل لتخزين المعلومات وخدمات) باستخدام هذه الأسماء المشتركة. وتعرف هذه التوصية استعمال CVE لتوفير آلية تسمح باستعمال قواعد بيانات مواطن الضعف والقدرات الأخرى مع بعضها البعض، وتسهيل مقارنة الأدوات والخدمات الأمنية. لا تتضمن CVE معلومات بشأن المخاطر أو الآثار أو معلومات لحل المشاكل أو معلومات تقنية مفصلة. فهي تتضمن فقط رقم معرف الهوية المعياري ومؤشر الحالة ووصفاً موجزاً وإحالات إلى تقارير ونشرات معلوماتية متصلة بمواطن الضعف. ومكان تخزين معرفات هوية المواطن CVE موجود في الموقع [cve.mitre.org/cve/cve.html]

ويُتوخى من CVE التي يرد تعريف استعمالها في هذه التوصية أن تكون شاملة لجميع مواطن الضعف والتعرض المعروفة لدى الجمهور. وفي حين صُممت المواطن CVE لتتضمن معلومات وافية، ينصبّ التركيز في المقام الأول على تحديد مواطن الضعف والتعرض التي تكشف عنها الأدوات الأمنية وأي مشاكل أخرى استجرت وأصبحت عامة، ثم على معالجة أي مشاكل أمنية أقدم تحتاج إلى التحقق.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرفة الهوية الفريد*
1.0	ITU-T X.1520	2011-04-20	17	11.1002/1000/11061
2.0	ITU-T X.1520	2014-01-24	17	11.1002/1000/12040

* للفاذ إلى التوصية، اطبع العنوان الإلكتروني <http://handle.itu.int/> في حقل العنوان بمتصفح الويب الذي تستعمله متبوعاً بمعرف الهوية الفريد للتوصية، وذلك كما يلي على سبيل المثال، <http://handle.itu.int/11.1002/1000/11830-en>.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريف، 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 الكهروتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها. والتقييد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقييد بهذه التوصية حاصلاً عندما يتم التقييد 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 التقييد 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع

<http://www.itu.int/ITU-T/ipr/>

© ITU 2014

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1	1
1	2
1	3
1	1.3
1	2.3
1	4
3	5
3	6
4	7
4	8
5	9
5	10
6	11
6	12
8	الملحق ألف - الشروط الخاصة بالنوع
10	الملحق باء - شروط الوسائط
11	الملحق جيم - شروط الوسائط
19	بيبلوغرافيا

تقدم التوصية التي تخصّ استعمال مواطن الضعف والتعرض الشائعة (CVE) وسيلةً منظّمة لتبادل المعلومات الأمنية بشأن مواطن الضعف والتعرض الشائعة، توفر أسماءً مشتركة للمشاكل التي يعرفها الجمهور. والهدف من هذه التوصية هو تعريف استعمال المواطن CVE من أجل زيادة تسهيل تبادل البيانات عبر قُدرات منفصلة لتحديد مواطن الضعف (أدوات ووسائل تخزين للمعلومات وخدمات) باستخدام هذه الأسماء المشتركة. وضمّمت هذه التوصية لتسمح باستعمال قواعد بيانات مواطن الضعف والقدرات الأخرى مع بعضها البعض، وتسهيل مقارنة الأدوات والخدمات الأمنية. ولا تتضمن المواطن CVE معلومات بشأن المخاطر أو الآثار أو معلومات لحل المشاكل أو معلومات تقنية مفصلة. فهي تتضمن فقط رقم معرّف الهوية المعياري ومؤشر الحالة ووصفاً موجزاً وإحالات إلى تقارير ونشرات معلوماتية متصلة بموطن الضعف. ومكان تخزين معرّفات هوية المواطن CVE موجود على الموقع <http://cve.mitre.org/cve/cve.html>.

ويُتوخى من المواطن CVE التي يرد تعريف استعمالها في هذه التوصية أن تكون شاملة لجميع مواطن الضعف والتعرض المعروفة لدى الجمهور. وفي حين صُمّمت هذه المواطن لتتضمن معلومات وافية، ينصبّ التركيز في المقام الأول على تحديد مواطن الضعف والتعرض التي تكشف عنها الأدوات الأمنية وأي مشاكل أخرى استُجدّت وأصبحت عامة، ثم على معالجة أي مشاكل أمنية أقدم تحتاج إلى التحقق.

وهذه التوصية واحدة من صنف توصيات قطاع تقييس الاتصالات التي تأتي من مجتمع حالي واسع للتنمية والمستخدمين على الصعيد العالمي، قام بكتابة وتطوير مواصفة مفتوحة معروضة على قطاع تقييس الاتصالات ليعتمدها مع الاتفاق على أن أي تغييرات أو تحديثات للمواصفة ستُجرى بأسلوب يضمن الحفاظ بشكل كامل على التكافؤ والتوافق التقنيين، وأن تُجرى المناقشات الخاصة بالتغييرات والتحسينات من خلال مجتمع المستخدمين الأصلي، على أن يشمل ذلك إحالات صريحة إلى الصيغة المحددة المقابلة التي يحتفظ بها مجتمع المستخدمين.

مواطن الضعف والتعرض الشائعة

1 مجال التطبيق

تقدم هذه التوصية التي تخص استعمال مواطن الضعف والتعرض الشائعة وسيلة منظّمة لتبادل المعلومات على المستوى العالمي بشأن مواطن الضعف والتعرض المدروسة المعروفة لدى الجمهور والتي تكشف عنها الوسائل الأمنية أو التي تصبح معروفة بوسائل أخرى. وهذه "الوسيلة المنظمة" يشار إليها عادة بمصطلح "توافق المواطن CVE" وتعرف الاستعمال السليم لهذه المواطن. وموطن الضعف في أمن المعلومات هو خطأ في البرمجيات يمكن أن يستخدمه بشكل مباشر أحد قرصنة الحاسوب من أجل النفاذ إلى نظام أو شبكة. أما موطن التعرض في أمن المعلومات فهو خطأ في البرمجيات يمكن من النفاذ إلى المعلومات أو القدرات التي يمكن أن يستخدمها هذا القرصان كنقطة انطلاق للدخول إلى نظام أو شبكة. ولا يغطي مجال تطبيق هذه التوصية تخصيص معرفات هوية مواطن الضعف والتعرض الشائعة.

أعدت التوصية ITU-T X.1520 بالتعاون مع مؤسسة MITRE، أخذاً في الاعتبار أهمية الحفاظ، قدر الإمكان، على التوافق التقني بين التوصية ITU-T X.1520 و"شروط وتوصيات توافق مواطن الضعف والتعرض الشائعة"، المؤرخة 30 يونيو 2013، المتاحة على https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf.

2 المراجع

لا توجد.

3 التعاريف

1.3 المصطلحات المعرّفة في توصيات أخرى

لا توجد.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

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

2.2.3 القدرة (capability): الأداة الأمنية أو قاعدة البيانات أو موقع الويب أو النشرة أو الخدمة التي تؤدي وظيفة التعرف على هوية موطن الضعف أو التعرض.

3.2.3 التعرض (exposure): موطن التعرض في أمن المعلومات هو خطأ في البرمجيات يمكن من النفاذ إلى المعلومات أو القدرات التي يمكن أن يستخدمها أحد قرصنة الحاسوب كنقطة انطلاق للدخول إلى نظام أو شبكة.

4.2.3 الخريطة/التقابل (map/mapping): تحديد العلاقات بين العناصر الأمنية في وسيلة تخزين وأسماء مواطن الضعف والتعرض الشائعة المرتبطة بهذه العناصر.

5.2.3 المالك (owner): القيم (شخص حقيقي أو شركة) المسؤول عن القدرة.

6.2.3 وسيلة التخزين (repository): مجموعة واضحة أو ضمنية من العناصر الأمنية، تدعم قدرة ما، مثل قاعدة بيانات خاصة بمواطن الضعف أو أرشيف للنشرات المعلوماتية أو مجموعة من التوقيعات في نظام لكشف الاقتحام أو موقع ويب.

- 7.2.3 **المراجعة (review):** عملية تحديد توافق أو عدم توافق قدرة ما إزاء مواطن الضعف والتعرض الشائعة.
- 8.2.3 **سلطة المراجعة (review authority):** أي كيان يقوم بإجراء مراجعة.
ملاحظة - شركة MITRE هي سلطة المراجعة الوحيدة حالياً.
- 9.2.3 **تاريخ المراجعة (review date):** تاريخ محتوى مواطن الضعف والتعرض الشائعة المستعمل لتحديد توافق قدرة ما إزاء مواطن الضعف والتعرض الشائعة.
- 10.2.3 **عينة المراجعة (review sample):** مجموعة العناصر الأمنية الموجودة في وسيلة التخزين الخاصة بالقدرة، التي تستخدمها سلطة المراجعة من أجل تقييم الدقة.
- 11.2.3 **أسلوب الاعتيان (sampling method):** الأسلوب الذي تحدد به سلطة المراجعة مجموعة العناصر الأمنية في عين المراجعة.
- 12.2.3 **حجم العينة (sample size):** النسبة المئوية و/أو عدد العناصر الأمنية التي تفحصها سلطة المراجعة.
- 13.2.3 **العنصر الأمني (security element):** سجل في قاعدة بيانات أو بريد إلكتروني أو نشرة معلوماتية أمنية أو مسبار تقييم أو توقيع أو أي عنصر آخر، مرتبط بموطن ضعف أو تعرض محدد.
- 14.2.3 **المهمة (task):** مسبار أداة أو تفحص أو توقيع أو عنصر آخر، يؤدي عملاً معيناً ينتج المعلومات الأمنية (أي العناصر الأمنية).
- 15.2.3 **الأداة (tool):** تطبيق برمجيات أو جهاز يفحص مستضيفاً أو شبكة وينتج المعلومات المرتبطة بمواطن الضعف أو التعرض أو يقوم بتجميع هذا النوع من المعلومات، مثل مسح مواطن الضعف أو نظام كشف الاقتحام أو إدارة للمخاطر أو إدارة المعلومات الأمنية أو أداة أو خدمة الإبلاغ بشأن الامتثال.
- 16.2.3 **المستعمل (user):** مستهلك للقدرة أو مستهلك محتمل لها.
- 17.2.3 **موطن الضعف (vulnerability):** أي ضعف في برمجية يمكن استغلاله في انتهاك نظام أو ما يتضمّنه من معلومات (استناداً إلى التوصية [b-ITU-T X.1500]).

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

النظام الأمريكي الموحد لتبادل المعلومات (American Standard Code for Information Interchange)	ASCII
مواطن الضعف والتعرض الشائعة (Common Vulnerabilities and Exposures)	CVE
السطح البيئي البياني للمستعمل (Graphical User Interface)	GUI
لغة وسم النصوص الفائقة (HyperText Markup Language)	HTML
بروتوكول نقل النص الفائق (HyperText Transfer Protocol)	HTTP
نظام كشف الاقتحام (Intrusion Detection System)	IDS
نسق الوثائق المحمولة (Portable Document Format)	PDF
جهة الاتصال (Point Of Contact)	POC
موقع الموارد الموحد (Uniform Resource Locator)	URL
لغة الوسم القابلة للتوسيع (Extensible Markup Language)	XML

يستخدم المختصر CVE في هذه التوصية كاسم.

6 الشروط رفيعة المستوى

تعرف البنود التالية المفاهيم والأدوار والمسؤوليات المتعلقة بالاستعمال السليم لمعرفات هوية المواطن CVE لتبادل البيانات عبر قدرات مواطن الضعف المنفصلة (أدوات، وسائل تخزين، وخدمات) لإفساح المجال أمام استعمال قواعد بيانات مواطن الضعف وغيرها من القدرات مع بعضها البعض ولتسهيل مقارنة الأدوات والخدمات الآمنة.

الشروط الأساسية

- 1.6 يجب أن يكون مالك القدرة كياناً قانونياً صحيحاً، أي منظمة أو شخص معين، وأن يكون في حوزته رقم هاتف صالح وعنوان بريدي إلكتروني وعنوان بريدي عادي.
- 2.6 ويجب أن تقدم القدرة قيمة أو معلومات إضافية تتعدى تلك المقدمة في مواطن الضعف والتعرض الشائعة نفسها (أي الاسم والوصف والمراجع والبيانات ذات الصلة).
- 3.6 ويجب أن يضع مالك القدرة رهن إشارة سلطة المراجعة نقطة اتصال تقنية مؤهلة للإجابة على الأسئلة المتصلة بالتقابل وأية وظيفة للقدرة متصلة بمواطن الضعف والتعرض الشائعة.
- 4.6 ويجب أن تكون القدرة متاحة للجمهور أو لمجموعة من المستهلكين في شكل منتج.
- 5.6 ويجب أن يقدم مالك القدرة لسلطة المراجعة "استمارة تقييم شروط التوافق إزاء مواطن الضعف والتعرض الشائعة"، تكون مكتملة.
- 6.6 وبالنسبة لقدرة ذات وسيلة تخزين، يجب أن يسمح مالك القدرة لسلطة المراجعة بالنفاذ الحر إلى وسيلة التخزين كي تستطيع هذه السلطة تحديد ما إذا كانت هذه الوسيلة تفي بجميع الشروط ذات الصلة.
- 7.6 وبالنسبة لقدرة ذات وسيلة تخزين، يجب أن يسمح مالك القدرة لسلطة المراجعة باستخدام هذه الوسيلة لتحديد أي مواطن ينبغي إضافتها إلى قائمة مواطن الضعف والتعرض الشائعة.
- 8.6 ويجب أن يوافق مالك القدرة على التقييد بجميع الشروط الإلزامية للتوافق إزاء مواطن الضعف والتعرض الشائعة، التي تشمل الشروط الإلزامية المتعلقة بهذا النوع من القدرة.

الوظيفة

- 9.6 يجب أن تسمح القدرة للمستخدمين بتحديد أماكن العناصر الأمنية التي تستخدم أسماء مواطن الضعف والتعرض الشائعة ("مواطن الضعف والتعرض الشائعة القابلة للبحث").
- 10.6 وعندما تقدم القدرة عناصر أمنية للمستخدم، يجب أن تسمح للمستخدم بالحصول على أسماء مواطن الضعف والتعرض الشائعة ذات الصلة ("نواتج مواطن الضعف والتعرض الشائعة").
- 11.6 وبالنسبة لقدرة ذات وسيلة تخزين، يجب أن يربط تقابل القدرة ربطاً دقيقاً العناصر الأمنية بالأسماء المناسبة لمواطن الضعف والتعرض الشائعة ("دقة التقابل").
- 12.6 ويجب أن تصف الوثائق المتعلقة بالقدرة وصفاً كافياً مواطن الضعف والتعرض الشائعة وتوافقها وطريقة استعمال الوظيفة المتصلة بها في القدرة ("وثائق القدرة").
- 13.6 ويجب أن تبين القدرة تاريخ سريانها فيما يخص مواطن الضعف والتعرض الشائعة ("تاريخ الاستعمال").

- 14.6 ويجب أن تفي القدرة بأية شروط إضافية خاصة بهذا النوع من القدرة، على النحو المحدد في الملحق ألف.
- 15.6 ويجب أن تفي القدرة بجميع شروط وسائط توزيعها، على النحو المحدد في الملحق باء.
- 16.6 ويجب ألا يُطلب من القدرة القيام بأي من الأمرين التاليين:
- استعمال الأوصاف أو المراجع نفسها على غرار مواطن الضعف والتعرض الشائعة
 - إدراج اسم كل موطن من مواطن الضعف والتعرض الشائعة في وسيلة التخزين الخاصة بها.

متفرقات

- 17.6 إذا لم تستوف القدرة جميع الشروط المطبقة (من 1.6 إلى 16.6 أعلاه)، فيجب ألا يعلن مالك القدرة أنها متوافقة إزاء مواطن الضعف والتعرض الشائعة.

7 الدقة

- توافق مواطن الضعف والتعرض الشائعة يسهل فقط تبادل البيانات إذا كان تقابل القدرة دقيقاً. ولهذا، يجب أن تفي القدرات المتوافقة من حيث مواطن الضعف والتعرض الشائعة بشروط الحد الأدنى للدقة الموضحة أدناه.
- 1.7 وبالنسبة لقدرة ذات وسيلة تخزين، يجب أن تبلغ نسبة دقة وسيلة التخزين 90 في المائة أو أكبر.
- 2.7 وخلال فترة المراجعة، يجب أن يصحح مالك القدرة أية أخطاء في التقابل تجدها سلطة المراجعة.
- 3.7 وبعد فترة المراجعة، ينبغي أن يصحح مالك القدرة أي خطأ في التقابل في غضون إطار زمني معقول بعد التاريخ الذي أشير فيه أول مرة إلى الخطأ، أي في غضون صيغتين (2) من صيغ وسيلة التخزين أو ستة (6) أشهر بالنسبة للأدوات وثلاثة (3) أشهر بالنسبة للقدرات والخدمات على الخط.
- 4.7 وبالنسبة لقدرة ذات وسيلة تخزين، ينبغي أن يعد ويوقع مالك القدرة بياناً يفيد فيه، وفقاً لأفضل ما هو متوافر لديه من معرفة، بأنه ما من أخطاء في التقابل.
- 5.7 وإذا كانت القدرة تستند إلى قدرة أخرى متوافقة من حيث مواطن الضعف والتعرض الشائعة أو تستعملها (القدرة "المصدر")، وأصبح مالك القدرة مدركاً لأخطاء التقابل في القدرة المصدر، فيجب أن يرفع مالك القدرة تقريراً بشأن هذه الأخطاء إلى مالك القدرة المصدر.
- 6.7 ويجب أن يجري التحقق من دقة التقابل فيما يخص أرشيفات النشرات المعلوماتية مقابل جميع العناصر الأمنية لوسيلة التخزين الخاصة بالأرشيف التالي التي تشمل استعمال الأرشيف لاسم أحد مواطن الضعف والتعرض الشائعة في عنصر أمني للمرة الأولى.
- 7.7 يجب أن تُظهر أي قدرة حالة أسماء مواطن الضعف والتعرض الشائعة الملغاة في غضون ثلاثة (3) أشهر من أجل القدرات والخدمات على الخط.
- 8.7 يجب ألا تُنتج أي قدرة معرفّات هوية ملغاة للمواطن CVE عندما يتم تحديد معرفّات هوية أكثر ملاءمة في وصف معرفّات الهوية الملغاة للمواطن CVE في غضون ثلاثة (3) أشهر من إلغاء معرفّات هوية المواطن CVE.

8 الوثائق

تنطبق الشروط التالية على الوثائق التي تُقدّم مع القدرة.

- 1.8 يجب أن تتضمن الوثائق وصفاً موجزاً لمواطن الضعف والتعرض الشائعة وتوافق هذه المواطن، حيث يمكن أن يستند إلى أجزاء حرفية من الوثائق المودعة على موقع الويب الخاص بمواطن الضعف والتعرض الشائعة.
- 2.8 ويجب أن تصف الوثائق الطريقة التي يمكن أن يجد بها المستعمل عناصر أمنية فردية في وسيلة التخزين الخاصة بالقدرة عن طريق استعمال أسماء مواطن الضعف والتعرض الشائعة.

3.8 ويجب أن تصف الوثائق الطريقة التي يمكن أن يحصل بها المستعمل على أسماء مواطن الضعف والتعرض الشائعة انطلاقاً من عناصر فردية في وسيلة التخزين الخاصة بالقدرة.

4.8 وإذا كانت الوثائق تتضمن فهرساً، فينبغي أن تشمل إحالات إلى الوثائق المتصلة بمواطن الضعف والتعرض الشائعة تحت مصطلح "مواطن الضعف والتعرض الشائعة".

9 تاريخ استعمال مواطن الضعف والتعرض الشائعة

يجب أن يكون المستعملون قادرين على تحديد حالة "تحديث" وسيلة التخزين الخاصة بقدرة ما فيما يخص تقابلها مع مواطن الضعف والتعرض الشائعة. ولا بد أن يبين مالك القدرة سريان التقابل من خلال ذكر تاريخ آخر تحديث قام به بشأن معلومات مواطن الضعف والتعرض الشائعة، وأن يبين الجزء الذي استخدمه من محتوى مواطن الضعف والتعرض الشائعة والمكان الذي يجمع منه محتوى مواطن الضعف والتعرض الشائعة هذا.

1.9 ويجب أن تحدد كل صيغة جديدة للقدرة التاريخ الأحدث لمحتوى مواطن الضعف والتعرض الشائعة الذي استخدم في وضع أو تحديث التقابل من خلال واحد على الأقل من الأمور التالية: تغيير السجلات أو قوائم السمات الجديدة أو ملفات المساعدة أو بعض الآليات الأخرى. وتكون القدرة "محدّثة" بالنسبة لذلك التاريخ.

2.9 ويجب أن تكون كل صيغة جديدة للقدرة محدّثة بالنسبة لتاريخ مبين لمواطن الضعف والتعرض الشائعة لا يتعدى ثلاثة (3) أشهر قبل إتاحة القدرة لمستعمليها. وإذا لم تستوف قدرة ما هذا الشرط، فإنها تكون "متقدمة" حسب التعريف.

3.9 ويجب أن يعلن مالك القدرة عن السرعة التي سيحدّث بها وسيلة التخزين الخاصة بالقدرة ليشمل المعلومات الجديدة عن مواطن الضعف والتعرض الشائعة.

4.9 ويجب أن يصف مالك القدرة معايير وآلية انتقاء المعلومات المتعلقة بمواطن الضعف والتعرض الشائعة التي يدرجها في قدرته.

5.9 ويجب أن يصف مالك القدرة المصدر الذي يجمع منه محتوى مواطن الضعف والتعرض الشائعة الجديد.

10 دعم مختلف أشكال اسم مواطن الضعف والتعرض الشائعة

يجب أن تعمل أي قدرة بأسماء لمواطن الضعف والتعرض الشائعة، بغض النظر عن نسق عرض الاسم في القدرة، سواء استخدمت قواعد التركيب CVE-ID من النمط الأقدم بأربعة أرقام أو قواعد التركيب CVE-ID متغيرة الطول (أربعة أرقام أو أكثر) (يتم استخدامها بعد تعديل قواعد التركيب CVE-ID بعد 30 ديسمبر 2013).

1.10 إذا قام مستعمل يبحث مستخدماً YYYYY-NNNNN أو YYYYY-NNNNN أو YYYYY-NNNNN أو أي معرفات هوية أخرى صالحة ذات عدد أكبر من الأرقام، فيجب أن تعيد القدرة العناصر الأمنية التي تقابل CVE-YYYY-NNNN أو CVE-YYYY-NNNNN أو أي معرفات هوية أخرى سارية ذات عدد أكبر من الأرقام على التوالي، بغض النظر عما إذا كان اسم موطن الضعف والتعرض الشائع يتضمن CVE أو CAN كجزء منه، في وسيلة التخزين الخاصة بالقدرة.

2.10 وإذا تضمنت القدرة اسم موطن الضعف والتعرض الشائع CVE-YYYY-NNNN، في حين يقوم المستعمل بالبحث مستخدماً النسق القديم لاسم موطن الضعف والتعرض الشائع CAN-YYYY-NNNN (المستخدم قبل تعديل مخطط تسمية مواطن الضعف والتعرض الشائعة الذي أجري في 19 أكتوبر 2005)، فينبغي للقدرة حينها أن تعيد CVE-YYYY-NNNN.

11 إلغاء توافق مواطن الضعف والتعرض الشائعة

- 1.11 إذا تحققت سلطة مراجعة من توافق قدرة إزاء مواطن الضعف والتعرض الشائعة، لكن أدلة بينت لسلطة المراجعة في وقت لاحق أن الشروط غير مستوفاة، فيجوز لهذه السلطة حينئذ أن تلغي تصديقها.
- 1.1.11 ويجب أن تحدد سلطة المراجعة الشروط المحددة غير المستوفاة.
- 2.11 ويجب أن تحدد السلطة ما إذا كانت إجراءات أو ادعاءات مالك القدرة "مضللة عن قصد".
- 1.2.11 ويجوز لسلطة المراجعة أن تفسر جملة "مضللة عن قصد" على النحو الذي تريده.
- 3.11 وينبغي ألا تنظر سلطة المراجعة في إلغاء التوافق من حيث مواطن الضعف والتعرض الشائعة لقدرة معينة أكثر من مرة واحدة في كل ستة (6) أشهر، إلا إذا أوصى بغير ذلك عضوان من هيئة التحرير الخاصة بمواطن الضعف والتعرض الشائعة، تكون مصالحهما غير متضاربة.

التحذير والتقييم

- 4.11 يجب أن تقدم سلطة المراجعة إلى مالك القدرة أو جهة الاتصال التقنية (POC) تحذيراً بالإلغاء قبل الوقت المزمع إجراء الإلغاء فيه بشهرين (2) على الأقل.
- 1.4.11 وإذا اكتشفت سلطة المراجعة أن إجراءات أو ادعاءات مالك القدرة مضللة عن قصد، فيجوز لهذه السلطة تخطي فترة التحذير.
- 5.11 وإذا كان مالك القدرة يرى أن الشروط مستوفاة، فيجوز له أن يرد على تحذير الإلغاء بتقديم تفاصيل محددة تبين لماذا يرى أن القدرة مستوفاة للشروط المقصودة.
- 6.11 وإذا قام مالك القدرة بتعديل القدرة لكي تتقيد بالشروط المقصودة خلال فترة التحذير، فينبغي لسلطة المراجعة إنهاء إجراء الإلغاء بالنسبة للقدرة.

الإلغاء

- 7.11 يجوز لسلطة المراجعة أن تؤجل تاريخ الإلغاء.
- 8.11 ويجب أن تعلن سلطة المراجعة أن التوافق من حيث مواطن الضعف والتعرض الشائعة قد ألغي بالنسبة للقدرة.
- 9.11 وإذا وجدت سلطة المراجعة أن إجراءات مالك القدرة فيما يتعلق بشروط التوافق من حيث مواطن الضعف والتعرض الشائعة مضللة بشكل مقصود، فينبغي أن يدوم الإلغاء سنة واحدة على الأقل.
- 10.11 ويجوز لسلطة المراجعة إعلان سبب الإلغاء.
- 11.11 وإذا أُلغي التصديق، لا يجوز لمالك القدرة طلب إجراء مراجعة جديدة خلال فترة الإلغاء.

12 سلطة المراجعة

فيما يخص أي مراجعة تجريها سلطة المراجعة:

- 1.12 يجب أن تراجع سلطة المراجعة القدرة لتحديد التوافق من حيث مواطن الضعف والتعرض الشائعة فيما يخص تاريخ محتوى معين لمواطن الضعف والتعرض الشائعة، أي تاريخ المراجعة.
- 2.12 ويجب أن تحدد سلطة المراجعة بشكل واضح تاريخ المراجعة الذي استعمل من أجل تحديد توافق القدرة.

- 3.12** ويجب أن تحدد سلطة المراجعة بشكل واضح صيغة وثيقة شروط التوافق من حيث مواطن الضعف والتعرض الشائعة، التي استُخدمت من أجل تحديد توافق القدرة.
- 4.12** ويجب أن تحدد وتنشر سلطة المراجعة حجم العينة.
- 1.4.12** وينبغي أن تستخدم سلطة المراجعة حجم عينة يشمل 50 عنصراً إضافة إلى 5 في المائة من وسيلة تخزين القدرة، وبحيث يصل حجم العينة إلى 400 عنصر كحد أقصى.
- 2.4.12** ويجوز لسلطة المراجعة أن تراجع كل عنصر في وسيلة تخزين القدرة.
- 5.12** ويجب أن تعلن سلطة المراجعة أسلوب الاعتيان.
- 6.12** ويجوز لسلطة المراجعة أن تستعمل عينة مراجعة لم يتم اختيارها عشوائياً.
- 7.12** ويجب أن تستخدم سلطة المراجعة أسلوب الاعتيان نفسه وحجم العينة نفسه بالنسبة لجميع القدرات التي تقيّم ضمن الإطار الزمني نفسه.

الملحق ألف

الشروط الخاصة بالنوع

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

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

ألف-1 ويجب أن تستوفي القدرة جميع الشروط الإضافية التي تتصل بنوع معين من أنواع القدرات.

ألف-1.1 وإذا كانت القدرة ماسحاً لتقييم مواطن الضعف والتعرض الشائعة، أو نظاماً للكشف عن الاقتحام، أو منتجاً يجمع نتائج واحد أو أكثر من أجهزة المسح وأنظمة الكشف عن الاقتحام، فيجب أن تستوفي القدرة شروط الأداة، ألف-1.2 إلى ألف-8.2.

ألف-2.1 وإذا كانت القدرة خدمة (مثل خدمة مدارة للكشف عن الاقتحام والتصدي له، أو خدمة مسح عن بُعد)، فيجب أن تستوفي شروط الخدمة الأمنية، ألف-1.3 إلى ألف-5.3.

ألف-3.1 وإذا كانت القدرة قاعدة بيانات لمواطن الضعف أو للتوقعات على الخط، أو أرشيف قائم على شبكة الويب، أو موقع إلكتروني للصيانة/الإصلاح، فيجب أن تستوفي شروط القدرة على الخط، ألف-1.4 إلى ألف-3.4.

ألف-4.1 وإذا كانت القدرة أداة تجميع مثل مدير للمعلومات الأمنية، أو أداة لتقديم تقارير بشأن الامتثال أو خدمة لإمداد هذه الأنواع من تجميعات المعلومات المتعلقة بأنواع مواطن الضعف، فيجب أن تستوفي شروط قدرة التجميع، ألف-1.5 إلى ألف-6.5.

شروط الأداة

ألف-1.2 يجب أن تسمح الأداة للمستعمل باستخدام أسماء مواطن الضعف والتعرض الشائعة لتحديد مواقع المهام ذات الصلة في تلك الأداة ("مواطن الضعف والتعرض 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 وأسماء مواطن الضعف والتعرض الشائعة الخاصة بها أو آلية أخرى.

ألف-2.2 وبالنسبة لأي تقرير يعرّف عناصر أمنية فردية، يجب أن تسمح الأداة للمستعمل بتحديد أسماء مواطن الضعف والتعرض الشائعة ذات الصلة بهذه العناصر ("نواتج مواطن الضعف والتعرض الشائعة") من خلال القيام بواحد على الأقل من الأمور التالية: إدراج أسماء مواطن الضعف والتعرض الشائعة بشكل مباشر في التقرير أو تقديم تقابل بين أسماء مهام الأداة وأسماء مواطن الضعف والتعرض الشائعة أو استعمال آلية أخرى.

ألف-3.2 ويجب أن تستوفي أية تقارير أو تقابلات مطلوبة شروط الوسائط على النحو المحدد في الملحق باء.

ألف-4.2 وينبغي للأداة أو مالك القدرة تزويد المستعمل بقائمة تضم جميع أسماء مواطن الضعف والتعرض الشائعة التي تتصل بمهام الأداة.

ألف-5.2 وينبغي أن تسمح الأداة للمستعمل بانتقاء مجموعة من المهام من خلال تقديم ملف يتضمن قائمة بأسماء مواطن الضعف والتعرض الشائعة.

ألف-6.2 وينبغي للسطح البيئي للأداة أن يسمح للمستعمل بتصفح وانتقاء وعدم انتقاء مجموعة من المهام باستخدام أسماء فردية لمواطن الضعف والتعرض الشائعة.

ألف-7.2 وإذا لم يكن للأداة مهمة تتصل باسم من أسماء مواطن الضعف والتعرض الشائعة يحدده المستعمل على النحو الوارد في شرطي الأداة ألف-5.2 أو ألف-6.2، ينبغي للأداة إخبار المستعمل بأنها لا تستطيع إنجاز المهمة ذات الصلة.

ألف-8.2 ويجب 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 وقع حدث متصل بعنصر أمني محدد، فإن الأداة تُخبر في بعض الأحيان بوقوع هذا الحدث.

شروط الخدمة الأمنية

يمكن للخدمات الأمنية استخدام الأدوات المتوافقة من حيث مواطن الضعف والتعرض 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.

ألف-1.3 يجب أن تكون الخدمة الأمنية قادرة على استعمال أسماء مواطن الضعف والتعرض الشائعة لإخبار المستعمل بشأن العناصر الأمنية التي اختبرتها الخدمة أو كشفت عنها ("مواطن الضعف والتعرض الشائعة القابلة للبحث") من خلال القيام بواحد أو أكثر من الأمور التالية: تزويد المستعمل بقائمة تضم أسماء مواطن الضعف والتعرض الشائعة وتحديد العناصر التي اختبرتها الخدمة أو كشفت عنها، أو تزويد المستعمل بتقابل بين عناصر الخدمة وأسماء مواطن الضعف والتعرض الشائعة، أو الرد على قائمة واردة من المستعمل بأسماء مواطن الضعف والتعرض الشائعة من خلال تحديد أسماء مواطن الضعف والتعرض الشائعة التي اختبرتها الخدمة أو كشفت عنها، أو استخدام آلية أخرى.

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

ألف-3.3 ويجب أن تستوفي أية تقارير أو تقابلات مطلوبة تقدمها الخدمة شروط الوسائط على النحو المحدد في الملحق باء.

ألف-4.3 وإذا كانت الخدمة تسمح للمستعمل بالنفاذ المباشر إلى منتج يعرّف عناصر أمنية، فينبغي أن يكون ذلك المنتج متوافقاً من حيث مواطن الضعف والتعرض الشائعة.

ألف-5.3 ويجب أن يضمن مالك القدرة 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.

شروط القدرة على الخط

ألف-1.4 يجب أن تسمح القدرة على الخط للمستعمل بالحصول على العناصر الأمنية ذات الصلة من وسيلة تخزين القدرة الموجودة على الخط ("مواطن الضعف والتعرض الشائعة القابلة للبحث") من خلال توفير أحد الأمور التالية: وظيفة للبحث تستعيد أسماء مواطن الضعف والتعرض الشائعة بالنسبة للعناصر ذات الصلة، أو تقابل يربط كل عنصر بالاسم المرتبط به من أسماء مواطن الضعف والتعرض الشائعة أو آلية أخرى.

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

أمثلة: <http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNN>

<http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNN>

<http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNNN>

<http://www.example.com/cve/CVE-YYYY-NNNN.html>

<http://www.example.com/cve/CVE-YYYY-NNNNN.html>

<http://www.example.com/cve/CVE-YYYY-NNNNNN.html>

ألف-2.1.4 وإذا كان نموذج موقع الموارد الموحد من أجل برنامج CGI، فينبغي أن يقبل البرنامج أسلوب "GET" لبروتوكول نقل النص الفائق.

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

ألف-3.4 وإذا كانت القدرة على الخط لا تقدم تفاصيل بشأن عناصر أمنية فردية، فيجب أن تقدم تقابلاً يربط كل عنصر بالاسم المتصل به من أسماء مواطن الضعف والتعرض الشائعة.

شروط قدرة التجميع

ألف-1.5 يجب أن تسمح قدرة التجميع للمستعمل باستخدام أسماء مواطن الضعف والتعرض الشائعة لتحديد مواقع العناصر ذات الصلة في تلك القدرة ("مواطن الضعف والتعرض الشائعة القابلة للبحث") من خلال توفير واحد على الأقل من الأمور التالية: وظيفة إيجاد "Find" أو بحث "Search" أو تقابل بين أسماء تلك القدرة وأسماء مواطن الضعف والتعرض الشائعة أو آلية أخرى توافق عليها سلطة المراجعة.

ألف-2.5 وبالنسبة لأي تقرير يعرّف عناصر أمنية فردية، يجب أن تسمح قدرة التجميع للمستعمل بتحديد أسماء مواطن الضعف والتعرض الشائعة ذات الصلة بالنسبة لهذه العناصر ("نواتج مواطن الضعف والتعرض الشائعة") من خلال القيام بواحد على الأقل من الأمور التالية: إدراج أسماء مواطن الضعف والتعرض الشائعة بشكل مباشر في التقرير أو توفير تقابل بين أسماء القدرة وأسماء مواطن الضعف والتعرض الشائعة أو استعمال آلية أخرى.

ألف-3.5 ويجب أن تستوفي أية تقارير أو تقابلات مطلوبة شروط الوسائط على النحو المحدد في الملحق باء.

ألف-4.5 وينبغي للأداة أو مالك القدرة تزويد المستعمل بقائمة تضم جميع أسماء مواطن الضعف والتعرض الشائعة التي تتصل بمهام الأداة.

ألف-5.5 وينبغي أن تسمح الأداة للمستعمل بانتقاء مجموعة من المهام من خلال تقديم ملف يتضمن قائمة بمواطن الضعف والتعرض الشائعة.

ألف-6.5 وينبغي للسطح البيني للأداة أن يسمح للمستعمل بتصفح وانتقاء وعدم انتقاء مجموعة من المهام باستخدام أسماء فردية لمواطن الضعف والتعرض الشائعة.

الملحق باء

شروط الوسائط

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

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

باء-2 يجب أن يستوفي نسق الوسائط الشروط المحددة الخاصة به.

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

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

باء-2.3 وإذا كانت الوثيقة لا تقدم سوى أسماء أو عناوين قصيرة لعناصر فردية، فيجب أن تشمل قائمة بأسماء مواطن الضعف والتعرض الشائعة التي تتصل بتلك العناصر ("نواتج مواطن الضعف والتعرض الشائعة").

باء-3.3 وينبغي أن تشمل الوثيقة تقابلاً بين العناصر وأسماء مواطن الضعف والتعرض الشائعة، يدرج الصفحات المناسبة بالنسبة لكل عنصر.

السطح البيئي البياني للمستخدم (GUI)

باء-1.4 على السطح البيئي البياني للمستخدم أن يزود المستخدم بوظيفة للبحث تسمح له بإدخال اسم من أسماء مواطن الضعف والتعرض الشائعة واسترداد العناصر ذات الصلة ("مواطن الضعف والتعرض الشائعة القابلة للبحث").

باء-2.4 إذا كان السطح البيئي البياني للمستخدم يشمل تفاصيل بشأن عنصر فردي، فيجب أن يدرج اسم (أسماء) موطن (مواطن) الضعف والتعرض الشائع (الشائعة) التي تقابل ذلك العنصر ("نواتج مواطن الضعف والتعرض الشائعة"). وإذا لم يكن الأمر كذلك، فعلى السطح البيئي البياني للمستخدم أن يزود المستخدم بتقابل في نسق يستوفي الشرط باء-1.3 المتعلق بالوثائق الإلكترونية.

باء-3.4 وينبغي للسطح البيئي البياني للمستخدم أن يسمح للمستخدم بتصدير البيانات المتعلقة بمواطن الضعف والتعرض الشائعة أو النفاذ إلى هذه البيانات في نسق بديل يستوفي الشرط باء-1.3 المتعلق بالوثائق الإلكترونية.

الملحق جيم

شروط الوسائط

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

تُتاح المخططات الواردة في هذا الملحق لمواطن الضعف والتعرض الشائعة بلغة التشفير القابلة للتوسيع على الموقع التالي:
http://cve.mitre.org/schema/cve/cve_1.0.xsd وهي مستنسخة أدناه.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://cve.mitre.org/cve/downloads/1.0"
  targetNamespace="http://cve.mitre.org/cve/downloads/1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <!-- ***** -->
  <!-- Changelog: 1.0 - Initial version -->
  <!-- ***** -->
  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Simple schema that defines the format of the CVE List provided by MITRE
    </xsd:documentation>
  </xsd:annotation>

  <!-- ***** -->
  <!-- Start Item Element Definition -->
  <!-- ***** -->
  <xsd:element name="cve">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        cve is the top level element of the CVE List provided by MITRE.
        It represents holds all CVE Items.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="item" type="ItemType" minOccurs="1" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="schemaVersion" type="xsd:token" use="optional"/>
    </xsd:complexType>
  </xsd:element>

  <!-- ***** -->
  <!-- Simple Types -->
  <!-- ***** -->
  <!-- CUSTOM TYPE DEFINITIONS-->
  <xsd:simpleType name="typeEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="CAN"/>
      <xsd:enumeration value="CVE"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="statusEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Entry"/>
      <xsd:enumeration value="Candidate"/>
    </xsd:restriction>
  </xsd:simpleType>

  <!-- need to verify enumeration -->
  <xsd:simpleType name="simplePhaseEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Proposed"/>
    </xsd:restriction>
  </xsd:simpleType>
```

```

        <xsd:enumeration value="Interim"/>
        <xsd:enumeration value="Modified"/>
        <xsd:enumeration value="Assigned"/>
    </xsd:restriction>
</xsd:simpleType>

<!-- ***** -->
<!-- Complex Types -->
<!-- ***** -->
<xsd:complexType name="ItemType">
    <xsd:sequence>
        <xsd:element name="status" type="statusEnumType" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="phase" type="specificPhaseType" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="desc" type="xsd:string" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="refs" type="refsType" minOccurs="1" maxOccurs="1"/>
        <xsd:element name="votes" type="votesType" minOccurs="0" maxOccurs="1"/>
        <xsd:element name="comments" type="commentsType" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
    <!--Need to Verify Enumeration-->
    <xsd:attribute name="type" type="typeEnumType" use="required"/>
    <xsd:attribute name="name" type="xsd:token" use="required"/>
    <xsd:attribute name="seq" type="xsd:token" use="required"/>
</xsd:complexType>

<xsd:complexType name="commentsType">
    <xsd:sequence>
        <xsd:element name="comment" minOccurs="0" maxOccurs="unbounded">
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="voter" type="xsd:token" use="required"/>
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="votesType">
    <xsd:sequence>
        <xsd:element name="accept" minOccurs="0" maxOccurs="1">
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="count" type="xsd:token" use="required"/>
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="modify" minOccurs="0" maxOccurs="1">
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="count" type="xsd:token" use="required"/>
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="noop" minOccurs="0" maxOccurs="1">
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="count" type="xsd:token" use="required"/>
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="recast" minOccurs="0" maxOccurs="1">
            <xsd:complexType>
                <xsd:simpleContent>

```

```

        <xsd:extension base="xsd:string">
          <xsd:attribute name="count" type="xsd:token" use="required"/>
        </xsd:extension>
      </xsd:simpleContent>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="reject" minOccurs="0" maxOccurs="1">
    <xsd:complexType>
      <xsd:simpleContent>
        <xsd:extension base="xsd:string">
          <xsd:attribute name="count" type="xsd:token" use="required"/>
        </xsd:extension>
      </xsd:simpleContent>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="reviewing" minOccurs="0" maxOccurs="1">
    <xsd:complexType>
      <xsd:simpleContent>
        <xsd:extension base="xsd:string">
          <xsd:attribute name="count" type="xsd:token" use="required"/>
        </xsd:extension>
      </xsd:simpleContent>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="revote" minOccurs="0" maxOccurs="1">
    <xsd:complexType>
      <xsd:simpleContent>
        <xsd:extension base="xsd:string">
          <xsd:attribute name="count" type="xsd:token" use="required"/>
        </xsd:extension>
      </xsd:simpleContent>
    </xsd:complexType>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="specificPhaseType">
  <xsd:simpleContent>
    <xsd:extension base="simplePhaseEnumType">
      <xsd:attribute name="date" type="xsd:token" use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>

<xsd:complexType name="refsType">
  <xsd:annotation>
    <xsd:documentation>holds all hyperlink elements</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="ref" type="refType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="refType">
  <xsd:annotation>
    <xsd:documentation>Holds individual hyperlink element</xsd:documentation>
  </xsd:annotation>
  <xsd:simpleContent>
    <xsd:extension base="xsd:string">
      <xsd:attribute name="source" type="xsd:token" use="required"/>
      <xsd:attribute name="url" type="xsd:anyURI" use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
</xsd:schema>

```

بيليوغرافيا

[b-ITU-T X.1500] 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 للتعريف
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 (ISDN)
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	بناء الكبلات وغيرها من عناصر المنشآت الخارجية وإنشاؤها وحمايتها
السلسلة M	إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	صيانة الدارات الإذاعية الدولية لإرسال البرامج الصوتية والتلفزيونية
السلسلة O	مواصفات أجهزة القياس
السلسلة P	جودة الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	التراسل الإبراقى
السلسلة S	التجهيزات الانتهاية لخدمات الإبراق
السلسلة T	تجهيزات مطرافية للخدمات التلمانية
السلسلة U	التبديل الإبراقى
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 للمبرمجيات في أنظمة الاتصالات