الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1544

(2013/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني –
تبادل الأحداث/الحوادث العارضة/المعلومات الحدسية

تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC)

التوصيـــة ITU-T X.1544

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 عن 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.1544

تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC)

ملخص

التوصية ITU-T X.1544 هي مواصفة قائمة على لغتي XML/XSD للتعرف على أنماط الهجمات ووصفها وتعدادها. وتعد أنماط الهجمات آلية قوية لالتقاط منظور المهاجم وللإبلاغ عنه. وهي عبارة عن أوصاف لطرائق شائعة لاستغلال البرمجيات. وتُستخلص من مفهوم أنماط التصميم المطبقة في السياق الهدّام بدلاً من البنّاء والناتجة عن التحليل المتعمق لأمثلة استغلالية محددة في العالم الحقيقي. ويهدف تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC) إلى توفير كتيّب إرشادي لأنماط الهجمات يتاح للجمهور إلى جانب مخطط شامل ومنهجية تصنيف لها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1544	2013.04.26	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

إن التوصية بشأن تعداد أنماط الهجمات الشائعة وتصنيفها (CAPEC) هي مواصفة قائمة على لغتي XML/XSD للتعرف على أنماط الهجمات ووصفها وتعدادها. وتعد أنماط الهجمات آلية قوية لالتقاط منظور المهاجم وللإبلاغ عنه. وهي عبارة عن أوصاف لطرائق شائعة لاستغلال البرمجيات. وتُستخلص من مفهوم أنماط التصميم المطبقة في السياق الهدّام بدلاً من البنّاء والناتجة عن التحليل المتعمق لأمثلة استغلالية محددة في العالم الحقيقي. ويهدف تعداد أنماط الهجمات الشائعة وتصنيفها (CAPEC) إلى توفير كتيب إرشادي لأنماط الهجمات يتاح للجمهور إلى جانب مخطط شامل ومنهجية تصنيف لها.

ويتيح تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC) ما يلي:

- تقييس التقاط ووصف أنماط الهجمات
- جمع أنماط الهجمات المعروفة في تعداد متكامل يمكن أن يستفيد منه المجتمع
- تصنيف أنماط الهجمات بحيث يسهل على المستخدمين تحديد مجموعة فرعية تتناسب مع سياقهم من كامل التعداد
- ربط أنماط الهجمات بتعدادات نقاط الضعف الشائعة (CWE) التي تكون فعالة تجاهها من خلال إحالات صريحة.

وقد وضعت التوصية ITU-T X.1544 مع مراعاة أهمية الحفاظ، إلى أبعد حد ممكن، على التوافق التقني مع الإصدار 1.0 (version 1.0) من "*شروط وتوصيات التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC)*"، الذي نشرته الشركة MITRE في 30 أغسطس 2012 (https://capec.mitre.org/compatible/requirements_v1.0.html).

التوصيـــة ITU-T X.1544

تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC)

1 مجال التطبيق

تنص هذه التوصية على التبادل المنظم لأنماط الهجمات المتاحة للجمهور إلى جانب مخطط شامل ومنهجية تصنيف لها.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

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

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة وثائق أخرى:

1.1.3 سلطة المراجعة [b-ITU-T X.1520]: كيان يقوم بإجراء المراجعة.

ملاحظـــة – شركة MITRE هي سلطة المراجعة الوحيدة الموجودة حالياً.

2.1.3 مواطن التعرض [b-ITU-T X.1500]: أي ضعف في البرمجية يمكن استغلاله في انتهاك نظام ما أو المعلومات التي يتضمنها.

2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 النسبة المئوية للدقة (accuracy percentage): النسبة المئوية للعناصر الأمنية في عينة المراجعة التي تشير إلى معرفات الهوية الصحيحة لتعداد وتصنيف أنماط الهجمات الشائعة (CAPEC).

2.2.3 حالة هجوم (attack instance): هجوم محدد بالتفصيل ضد تطبيق أو نظام ويستهدف مواطن التعرض أو الضعف في ذلك النظام.

3.2.3 نمط الهجمات (attack pattern): تجريد لنُهُج الهجمات الشائعة التي تلاحظ عامة ضد التطبيقات أو الأنظمة (مثل حقن لغة SQL، أو هجوم لمتطفل بين طرفين، أو قرصنة الدورة، أو غير ذلك).

ملاحظـــة – ويمكن أن يكون لنمط واحد من الهجمات عدد كبير من حالات الهجوم المتنوعة التي يمكن ربطها به.

4.2.3 القدرة (capability): أداة التقييم أو أداة اختبار أمن التطبيقات الدينامية (DAST) أو أداة اختبار الاختراق أو أداة أطر الاستغلال أو أداة نمذجة التهديدات أو قاعدة البيانات أو موقع الويب أو النشرة أو الخدمة التي توفر معلومات عن حالات الهجوم وأنماطه.

5.2.3 الخريطة/التقابل (map/mapping): تحديد العلاقات بين عناصر أنماط الهجوم في وسيلة تخزين وبنود تعداد وتصنيف أنماط الهجمات الشائعة ذات الصلة بتلك العناصر.

6.2.3 المالك (owner) [طبقاً للتوصية b-ITU-T X.1520]: القيّم (شخص حقيقي أو شركة) المسؤول عن القدرة (كما هو معرف في هذه التوصية).

7.2.3 وسيلة التخزين (repository): مجموعة واضحة أو ضمنية من عناصر نمط الهجوم، تدعم قدرة ما، مثل قاعدة بيانات خاصة بأنماط الهجوم أو مجموعة من حالات الهجوم في أداة اختبار أمن التطبيقات الدينامية أو أحد مواقع الويب.

8.2.3 المراجعة (review): عملية تحديد توافق أو عدم توافق قدرة ما إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

9.2.3 صيغة المراجعة (review version): الصيغة المحددة التاريخ لتعداد وتصنيف أنماط الهجمات الشائعة والتي استعملت لتحديد توافق قدرة ما إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

10.2.3 العنصر الأمني (security element): سجل في قاعدة بيانات أو مسبار تقييم أو حالة هجوم أو استغلال أو حمولة نافعة أو أي عنصر آخر، مرتبط بنمط هجمات محدد.

11.2.3 المهمة (task): مسبار أداة أو تفحص أو توقيع أو عنصر آخر، يؤدي عملاً معيناً ينتج المعلومات الأمنية (أي العناصر الأمنية).

12.2.3 الأداة (tool): تطبيق برمجيات أو جهاز يفحص الخصائص الأمنية لتطبيق أو نظام بواسطة المحاكاة أو المضاهاة أو تحديد خصائص الهجمات المحتملة ضد ذلك النظام، مثل أداة التقييم أو أداة اختبار أمن التطبيقات الدينامية (DAST) أو أداة اختبار الاختراق أو أداة أطر الاستغلال أو أداة نمذجة التهديدات.

13.2.3 المستعمل (user) [طبقاً للتوصية b-ITU-T X.1520]: مستهلك للقدرة أو مستهلك محتمل لها (كما هو معرف في هذه التوصية).

14.2.3 موطن الضعف (weakness): قصور أو نقص في شفرة البرامج أو التصميم أو المعمارية أو الانتشار يمكن أن يتحول في وقت ما إلى موطن تعرض أو يمكن أن يساهم في إدخال مواطن تعرض أخرى.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

CAPEC تعداد وتصنيف أنماط الهجمات الشائعة (*Common Attack Pattern Enumeration and Classification*)

CCR تمثيل الادعاء بالتغطية (*Coverage Claim Representation*)

CIA السرّية أو الحصانة أو التيسّر (*Confidentiality, Integrity or Availability*)

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

DAST أداة اختبار أمن التطبيقات الدينامية (*dynamic application security testing tool*)

GUI سطح بيني بياني للمستعمل (*Graphical User Interface*)

IDS نظام كشف الاقتحام (*Intrusion Detection System*)

POC جهة الاتصال (*Point Of Contact*)

5 الاصطلاحات

تُفسر الكلمات الأساسية "يتعين" و"يجب" و"لا يجب" و"ينبغي" و"لا ينبغي" و"الموصى به" و"يجوز" و"اختياري" في هذه التوصية، وفقاً للدليل المؤلف للاتحاد الدولي للاتصالات (متاح على http://www.itu.int/oth/T0A0F000004/en).

6 الشروط رفيعة المستوى

تعرِّف البنود التالية المفاهيم والأدوار والمسؤوليات المتعلقة بالاستعمال السليم لمعرّفات هوية تعداد وتصنيف أنماط الهجمات الشائعة (CAPEC) لتبادل البيانات عبر قدرات اختبار الأمن المنفصلة (أدوات، وسائل تخزين، خدمات) لإفساح المجال أمام استعمال قدرات اختبار الأمن هذه مع بعضها البعض ولتسهيل مقارنة أدوات وخدمات اختبار الأمن.

الشروط الأساسية

1.6 يجب أن يكون مالك القدرة كياناً قانونياً صحيحاً، أي منظمة أو شخصاً معيناً، 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 تعداد وتصنيف أنماط الهجمات الشائعة نفسها (أي الاسم والوصف والمخاطر والمراجع والمعلومات ذات الصلة عن مواطن الضعف).

3.6 ويجب أن يضع مالك القدرة رهن إشارة سلطة المراجعة نقطة اتصال تقنية مؤهلة للإجابة على الأسئلة المتصلة بالتقابل وأية وظيفة للقدرة متصلة بتعداد وتصنيف أنماط الهجمات الشائعة.

4.6 ويجب أن تكون القدرة متاحة للجمهور أو لمجموعة من المستهلكين في شكل منتج أو طبعة عامة.

5.6 ويجب أن يقدم مالك القدرة لسلطة المراجعة "استمارة تقييم شروط التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة"، تكون مكتملة.

6.6 ويجب أن يسمح مالك القدرة لسلطة المراجعة بالنفاذ الحر إلى وسيلة التخزين كي تستطيع هذه السلطة تحديد ما إذا كانت هذه الوسيلة تفي بجميع شروط دقة التقابل المرتبطة بها.

7.6 ويجب أن يسمح مالك القدرة لسلطة المراجعة باستخدام وسيلة التخزين لتحديد أي أنماط هجمات ينبغي إضافتها إلى تعداد وتصنيف أنماط الهجمات الشائعة.

8.6 ويجب أن يوافق مالك القدرة على التقيّد بجميع الشروط الإلزامية للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، التي تشمل الشروط الإلزامية المتعلقة بهذا النوع من القدرة.

الوظيفة

9.6 بالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، يجب أن تسمح القدرة للمستعملين بتحديد أماكن العناصر الأمنية التي تستخدم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة ("تعداد وتصنيف أنماط الهجمات الشائعة القابلة للبحث").

10.6 وبالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، عندما تقدم القدرة عناصر أمنية للمستعمل، يجب أن تسمح للمستعمل بالحصول على معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة ذات الصلة ("نواتج تعداد وتصنيف أنماط الهجمات الشائعة").

11.6 وبالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، يجب أن يربط تقابل القدرة ربطاً دقيقاً العناصر الأمنية بمعرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة ("دقة التقابل").

12.6 وبالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، يجب أن تصف الوثائق المتعلقة بالقدرة وصفاً كافياً تعداد وتصنيف أنماط الهجمات الشائعة وتوافقها وطريقة استعمال الوظيفة المتصلة بها في القدرة ("وثائق تعداد وتصنيف أنماط الهجمات الشائعة").

13.6 وبالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، يجب أن تدرِج وثائق القدرة المتاحة للجمهور صراحة قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي يعتبرها مالكُ القدرة أنها القدرة على تغطية جزء من وظيفتها ("تغطية تعداد وتصنيف أنماط الهجمات الشائعة").

14.6 وبالنسبة للتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، ينبغي على موقع القدرة على الويب المتاح للجمهور أن يقدم تغطية تعداد وتصنيف أنماط الهجمات الشائعة بشكل وثائق بلغة XML لتمثيل الادعاء بتغطية تعداد وتصنيف أنماط الهجمات الشائعة.

15.6 ويجب أن تدل القدرة على الصيغة المستعملة والمحددة التاريخ لتعداد وتصنيف أنماط الهجمات الشائعة (استعمال تعداد وتصنيف أنماط الهجمات الشائعة).

16.6 ويجب أن تفي القدرة بأي شروط إضافية للنوع المحدد للقدرة، على النحو المحدد في الملحق A.

17.6 ويجب أن تفي القدرة بجميع شروط وسائط توزيعها، على النحو المحدد في الملحق B.

18.6 ويجب ألا يُطلب من القدرة القيام بأي من الأمرين التاليين:

- استعمال الأوصاف أو المراجع نفسها على غرار تعداد وتصنيف أنماط الهجمات الشائعة؛
- إدراج معرف هوية لكل تعداد وتصنيف لأنماط الهجمات الشائعة في وسيلة التخزين الخاصة به.

متفرقات

19.6 إذا لم تستوفِ القدرة جميع الشروط المطبقة أعلاه (الفقرات من 1.6 إلى 18.6)، فيجب ألا يعلن مالك القدرة أنها متوافقة إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

7 الدقة

إن التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة يسهل فقط تبادل البيانات وترابطها إذا كان تقابل القدرة دقيقاً. ولذلك يجب أن تفي القدرات المتوافقة إزاء تعداد وتصنيف أنماط الهجمات الشائعة بشروط الحد الأدنى للدقة الموضحة أدناه.

1.7 يجب أن تبلغ نسبة دقة وسيلة التخزين 100 في المائة.

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 ضمن صيغتين (2) من صيغ وسيلة تخزين القدرة أو خلال (6) أشهر، أيهما أقصر.

4.7 وينبغي أن يعدّ 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 إزاء تعداد وتصنيف أنماط الهجمات 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.

8 الوثائق

تنطبق الشروط التالية على الوثائق التي تُقدَّم مع القدرة.

1.8 يجب أن تتضمن الوثائق وصفاً موجزاً لتعداد وتصنيف أنماط الهجمات الشائعة وتوافق هذا التعداد والتصنيف، حيث يمكن أن يستند إلى أجزاء حرفية من الوثائق المودعة على موقع الويب الخاص بتعداد وتصنيف أنماط الهجمات 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 معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة.

3.8 ويجب أن تصف الوثائق الطريقة التي يمكن أن يحصل بها المستعمل على معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة انطلاقاً من عناصر فردية في وسيلة التخزين الخاصة بالقدرة.

4.8 وإذا كانت الوثائق تتضمن فهرساً، فينبغي أن يشمل إحالات إلى الوثائق المتصلة بتعداد وتصنيف أنماط الهجمات الشائعة تحت مصطلح " تعداد وتصنيف أنماط الهجمات الشائعة".

9 استعمال صيغ تعداد وتصنيف أنماط الهجمات الشائعة

يجب أن يعرف المستعملون الصيغة الخاصة بتعداد وتصنيف أنماط الهجمات الشائعة التي يستعملونها في وسيلة التخزين الخاصة بقدرة ما فيما يخص تقابلها إزاء تعداد وتصنيف أنماط الهجمات الشائعة. ويمكن أن يبين مالك القدرة سريان التقابل من خلال ذكر صيغة تعداد وتصنيف أنماط الهجمات الشائعة أو تاريخ آخر تحديث أُجري للتقابل.

1.9 ويجب أن تحدد القدرة الصيغة الخاصة بتعداد وتصنيف أنماط الهجمات الشائعة، أو تاريخ تحديثها، التي استُخدمت في وضع أو تحديث التقابل من خلال واحد على الأقل من الأمور التالية: تغيير السجلات أو قوائم السمات الجديدة أو ملفات المساعدة أو إحدى الآليات الأخرى. وتكون القدرة "محدَّثة" بالنسبة لتلك الصيغة أو ذلك التاريخ.

2.9 وينبغي أن يتم تحديث كل صيغة جديدة للقدرة بالنسبة لصيغة تعداد وتصنيف أنماط الهجمات الشائعة التي صدرت قبل أربعة (4) أشهر على الأكثر من إتاحة القدرة لمستعمليها. وإذا لم تستوفِ قدرة ما هذا الشرط، فإنها تكون "متقادمة" حسب التعريف.

3.9 وينبغي أن يعلن مالك القدرة عن السرعة التي سيحدِّث بها وسيلة التخزين الخاصة بالقدرة بعد توفر صيغة جديدة أو تحديث لتعداد وتصنيف أنماط الهجمات الشائعة على موقع الويب الخاص بهذا التعداد والتصنيف.

10 إلغاء التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة

1.10 إذا تحققت سلطة مراجعة من توافق قدرة إزاء تعداد وتصنيف أنماط الهجمات الشائعة، لكن أدلة بينت لسلطة المراجعة في وقت لاحق أن الشروط غير مستوفاة، فيجوز لهذه السلطة حينئذ أن تلغي تصديقها.

1.1.10 ويجب أن تحدد سلطة المراجعة الشروط المحددة غير المستوفاة.

2.10 ويجب أن تحدد السلطة ما إذا كانت إجراءات أو ادعاءات مالك القدرة "مضلّلة عن قصد".

1.2.10 ويجوز لسلطة المراجعة أن تفسر جملة "مضللة عن قصد" على النحو الذي تريده.

3.10 وينبغي ألا تنظر سلطة المراجعة في إلغاء التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة لقدرة معينة أكثر من مرة واحدة في كل ستة (6) أشهر.

التحذير والتقييم

4.10 يجب أن تقدم سلطة المراجعة إلى مالك القدرة أو جهة الاتصال (POC) التقنية تحذيراً بالإلغاء قبل الوقت المزمع إجراء الإلغاء فيه بشهرين (2) على الأقل.

1.4.10 وإذا اكتشفت سلطة المراجعة أن إجراءات أو ادعاءات مالك القدرة مضللة عن قصد، فيجوز لهذه السلطة تخطي عدم التقيد بفترة التحذير.

5.10 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.

6.10 وإذا قام مالك القدرة بتعديل القدرة لكي تتقيد بالشروط المقصودة خلال فترة التحذير، فينبغي لسلطة المراجعة إنهاء إجراء الإلغاء بالنسبة للقدرة.

الإلغاء

7.10 يجوز لسلطة المراجعة أن تؤجل تاريخ الإلغاء.

8.10 ويجب أن تعلن سلطة المراجعة أن التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة قد ألغي بالنسبة للقدرة.

9.10 وإذا وجدت سلطة المراجعة أن إجراءات مالك القدرة فيما يتعلق بشروط التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة مضللة بشكل مقصود، فينبغي أن يدوم الإلغاء سنة واحدة على الأقل.

10.10 ويجوز لسلطة المراجعة إعلان سبب الإلغاء.

11.10 ويجوز لسلطة المراجعة نشر بيان عام متعلق بالإلغاء على الموقع نفسه.

12.10 وإذا أُلغي التصديق، **لا** يجوز لمالك القدرة طلب إجراء مراجعة جديدة خلال فترة الإلغاء.

11 سلطة المراجعة

1.11 يجب أن تراجع سلطة المراجعة القدرة لتحديد التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة فيما يخص صيغة محددة لتعداد وتصنيف أنماط الهجمات الشائعة، أي الصيغة المراجعة.

2.11 ويجب أن تحدد سلطة المراجعة بوضوح صيغة المراجعة التي استعملت من أجل تحديد توافق القدرة.

3.11 ويجب أن تحدد سلطة المراجعة بوضوح صيغة وثيقة شروط التوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة، التي استُخدمت من أجل تحديد توافق القدرة.

4.11 وينبغي أن تراجع سلطة المراجعة كل عنصر من عناصر مستودع التخزين بالنسبة لدقة التقابل مع تعداد وتصنيف أنماط الهجمات الشائعة.

5.11 وينبغي أن تراجع سلطة المراجعة قدرة ما بالنسبة للتقابل مع تعداد وتصنيف أنماط الهجمات الشائعة.

6.11 يجب أن تقدم سلطة المراجعة نسخة من استمارة إعلان التوافق CAPEC عند طلبها من مالك أي قدرة سارية يرغب في بدء عملية التوافق CAPEC.

7.11 يجب أن تقدم سلطة المراجعة نسخة من استمارة تقييم شروط التوافق CAPEC عند طلبها من مالك أي قدرة يقدم استمارة مستكملة لإعلان التوافق CAPEC.

الملحق A

الشروط الخاصة بالنوع

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

بما أن مجموعة واسعة من القدرات تستخدم تعداد وتصنيف أنماط الهجمات الشائعة، فقد تكون لدى أنواع معينة من القدرات سمات فريدة تستدعي اهتماماً خاصاً فيما يتعلق بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

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

1.1.A وإذا كانت القدرة أداة تقييم أو أداة اختبار أمن التطبيقات الدينامية (DAST) أو أداة اختبار الاختراق أو أداة أطر الاستغلال أو أداة نمذجة التهديدات أو منتجاً يجمع نتائج واحد أو أكثر من هذه الأنواع من الأجهزة، فيجب أن تستوفي القدرة شروط الأداة، الفقرات من 1.2.A إلى 8.2.A.

2.1.A وإذا كانت القدرة خدمة (مثل خدمة تقييم الأمن، أو خدمة اختبار الاختراق، أو خدمة تعليم أو تدريب)، فيجب أن تستوفي شروط الخدمة الأمنية، الفقرات من 1.3.A إلى 5.3.A.

3.1.A وإذا كانت القدرة قاعدة بيانات للهجمات المعروفة على الخط، أو مورداً قائم على شبكة الويب، أو موقعاً للمعلومات، فيجب أن تستوفي شروط القدرة على الخط، الفقرات من 1.4.A إلى 3.4.A.

2.A شروط الأداة

1.2.A يجب أن تسمح الأداة للمستعمل باستخدام معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة لتحديد مواقع المهام ذات الصلة في تلك الأداة ("تعداد وتصنيف أنماط الهجمات 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 تعداد وتصنيف أنماط الهجمات الشائعة الخاصة بها أو آلية أخرى تعتبر سلطة المراجعة أنها كافية.

2.2.A وبالنسبة لأي تقرير يعرِّف عناصر أمنية فردية، يجب أن تسمح الأداة للمستعمل بتحديد معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة ذات الصلة بهذه العناصر ("نواتج تعداد وتصنيف أنماط الهجمات الشائعة") من خلال القيام بواحد على الأقل من الأمور التالية: إدراج معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة بشكل مباشر في التقرير أو تقديم تقابل بين أسماء مهام الأداة وأسماء معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة أو استعمال آلية أخرى تعتبر سلطة المراجعة أنها كافية.

3.2.A ويجب أن تبين الوثائق المتاحة للجمهور صراحة قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي يعتبر مالك القدرة أنها الأداة الفعالة عند الشروع بالعمل ("تغطية الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة").

4.2.A ويمكن لموقع القدرة على الويب المتاح للجمهور أن يقدم تغطية بالادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة بشكل وثائق مكتوبة بلغة XML لتمثيل الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

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

6.2.A وينبغي للأداة أو مالك القدرة تزويد المستعمل بقائمة تضم جميع معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي تتصل بمهام الأداة.

7.2.A وينبغي أن تسمح الأداة للمستعمل بانتقاء مجموعة من المهام من خلال تقديم ملف يتضمن قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة.

8.2.A وينبغي للسطح البيني للأداة أن يسمح للمستعمل بتصفح وانتقاء وعدم انتقاء مجموعة من المهام باستخدام معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة.

9.2.A وإذا لم يكن للأداة مهمة تتصل بأحد معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة على النحو الوارد في شرطي الأداة في الفقرة 5.2.A أو الفقرة 6.2.A ، فينبغي للأداة إخبار المستعمل بأنها لا تستطيع إنجاز المهمة ذات الصلة.

3.A شروط الخدمة الأمنية

يمكن للخدمات الأمنية استخدام الأدوات المتوافقة مع تعداد وتصنيف أنماط الهجمات 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 قائمة

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

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

3.3.A ويجب أن تبين الوثائق المتاحة للجمهور صراحة قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي يعتبرها مالك القدرة أنها الخدمة الأمنية التي يجب تغطيتها بفعالية ("تغطية الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة").

4.3.A ويمكن لموقع القدرة على الويب المتاح للجمهور أن يقدم تغطية بالادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة بشكل وثائق مكتوبة بلغة XML لتمثيل الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

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

6.3.A وإذا كانت الخدمة توفر للمستعمل النفاذ المباشر إلى منتج يعرِّف عناصر أمنية، فينبغي أن يكون ذلك المنتج متوافقاً إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

4.A شروط القدرة 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 ("تعداد وتصنيف أنماط الهجمات الشائعة القابلة للبحث") من خلال توفير أحد الأمور التالية: وظيفة للبحث تستعيد معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة بالنسبة للعناصر ذات الصلة، أو تقابل يربط كل عنصر بأحد معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة أو آلية أخرى.

1.1.4.A 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 1.4.A، شروط القدرة على الخط.

أمثلة لروابط هامة:

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

2.1.4.A وإذا كان الموقع متاحاً للجمهور من دون تسجيل للدخول، فينبغي أن يقبل برنامج CGI أسلوب "GET" لبروتوكول نقل النص الفائق.

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

3.4.A ويجب أن تبين الوثائق المتاحة للجمهور صراحة قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي يعتبرها مالك القدرة أنها مستودع تخزين القدرة على الخط الذي يجب تغطيته ("تغطية الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة").

4.4.A ويمكن لموقع القدرة على الويب المتاح للجمهور أن يوفر تغطية الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة بشكل وثائق مكتوبة بلغة XML لتمثيل الادعاء بالتوافق إزاء تعداد وتصنيف أنماط الهجمات الشائعة.

5.4.A وإذا كانت القدرة على الخط لا تقدم تفاصيل بشأن عناصر أمنية فردية، فيجب أن تقدم تقابلاً يربط كل عنصر بمعرف الهوية المتصل به من معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة.

الملحق B

شروط الوسائط

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.B يجب أن تستخدم وسائط النشر التي تستخدمها قدرة متوافقة إزاء تعداد وتصنيف أنماط الهجمات 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" ("تعداد وتصنيف أنماط الهجمات الشائعة القابلة للبحث") مثل نصوص ASCII صرفة أو HTML أو PDF.

2.3.B وإذا كانت الوثيقة لا تقدم سوى أسماء أو عناوين قصيرة لعناصر فردية، فيجب أن تشمل قائمة تضم معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي تتصل بتلك العناصر ("نواتج تعداد وتصنيف أنماط الهجمات الشائعة").

3.3.B وينبغي أن تشمل الوثيقة تقابلاً بين العناصر ومعرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة، يدرج الصفحات المناسبة بالنسبة لكل عنصر.

4.B السطح البيني البياني للمستعمل

1.4.B على السطح البيني البياني للمستعمل (GUI) أن يزود المستعمل بوظيفة للبحث تسمح له بإدخال أحد معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة واسترداد العناصر ذات الصلة ("تعداد وتصنيف أنماط الهجمات الشائعة القابلة للبحث").

2.4.B إذا كان السطح البيني البياني للمستعمل يشمل تفاصيل بشأن عنصر فردي، فيجب أن يدرج معرفات هوية تعداد وتصنيف أنماط الهجمات الشائعة التي تقابل ذلك العنصر ("نواتج تعداد وتصنيف أنماط الهجمات الشائعة"). وإذا لم يكن الأمر كذلك، فعلى السطح البيني البياني للمستعمل أن يزود المستعمل بتقابل في نسق يستوفي الشروط المتعلقة بالوثائق الإلكترونية الواردة في الفقرة 1.3.B.

3.4.B وينبغي للسطح البيني البياني للمستعمل أن يسمح للمستعمل بتصدير البيانات المتعلقة بتعداد وتصنيف أنماط الهجمات الشائعة أو النفاذ إلى هذه البيانات في نسق بديل يستوفي الشروط المتعلقة بالوثائق الإلكترونية الواردة في الفقرة 1.3.B.

بيبليوغرافيا

[b-ITU-T X.1520] الوثيقة ITU–T X.1520 (2011)، *مواطِن الضعف والتعرّض الشائعة (CVE)*.

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

طُبعت في سويسرا
جنيف، 2013