|  |  |
| --- | --- |
| **مكتب تقييس الاتصالات** | logo_A-[Converted] |
|  |  |

|  |  |  |
| --- | --- | --- |
|  |  | جنيف، 27 سبتمبر 2012 |
| المرجع: | **TSB Circular 311**COM 17/MEU | * - إلى إدارات الدول الأعضاء في الاتحاد
 |
| الهاتف:الفاكس:البريد الإلكتروني: | +41 22 730 5866+41 22 730 5853tsbsg17@itu.int | **نسخة إلى:**- أعضاء قطاع تقييس الاتصالات؛- المنتسبين إلى قطاع تقييس الاتصالات؛- الهيئات الأكاديمية المنضمة إلى قطاع تقييس الاتصالات؛- رئيس لجنة الدراسات 17 ونوابه؛- مدير مكتب تنمية الاتصالات؛- مدير مكتب الاتصالات الراديوية |
|  |  |  |
| الموضوع: | **اجتماع لجنة الدراسات 17 بهدف الموافقة على مشاريع التوصيات الجديدة ITU‑T X.1126 وX.1154 وX.1526 وX.1544، عملاً بأحكام القسم 9 من القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات (جوهانسبرغ، 2008) جنيف، 26 أبريل 2013** |

حضرات السادة والسيدات،

تحية طيبة وبعد،

1 بناءً على طلب رئيس لجنة الدراسات 17، المعنية *بالأمن*، أتشرف بأن أُعلِمَكُم أن لجنة الدراسات هذه، التي ستجتمع من 17 إلى 26 أبريل 2013، تنوي تطبيق الإجراءات الموصوفة في القسم 9 من القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات (جوهانسبرغ، 2008) وذلك من أجل الموافقة على مشاريع التوصيات الجديدة المذكورة أعلاه.

2 ويشتمل **الملحق 1** بهذه الرسالة على ملخص مشاريع التوصيات الجديدة لقطاع تقييس الاتصالات المقترح الموافقة عليها، وعلى عناوينها والوثائق التي ترد فيها.

3 يرجى من أي دولة عضو في الاتحاد أو عضو في القطاع أو منتسب إليه أو هيئة أكاديمية، تعلم بوجود براءة اختراع في حيازتها أو في حيازة الغير من شأنها أن تشمل كلياً أو جزئياً عناصر من مشاريع التوصيات المقترح الموافقة عليها، أن تكشف عن مثل هذه المعلومات لمكتب تقييس الاتصالات، عملاً بالسياسة المشتركة للبراءات المعتمدة لدى قطاع تقييس الاتصالات/قطاع الاتصالات الراديوية/المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ITU-T/ITU-R/ISO/IEC).

ويمكن الاطلاع على معلومات براءات الاختراع المتاحة مباشرة على الخط في الموقع الإلكتروني للقطاع ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 وتبعاً لأحكام القسم 9 من القرار 1 سأكون ممتناً لو تفضلتم بإعلامي في موعد أقصاه منتصف الليل بالتوقيت العالمي المنسَّق **في 5 أبريل 2013** ما إذا كانت إدارتكم تفوِّض السلطة إلى لجنة الدراسات 17 للنظر في مشاريع هذه التوصيات الجديدة بغرض الموافقة عليها في اجتماع لجنة الدراسات.

وإذا رأت أي دولة عضو أن عملية النظر بغرض الموافقة ينبغي ألاّ تستمر فعليها أن تبيّن أسباب ذلك الاعتراض وأن تشير إلى التغييرات الممكنة التي من شأنها تيسير مواصلة النظر في مشاريع التوصيات الجديدة والموافقة عليها.

5 فإذا كان 70 في المائة أو أكثر من الردود الواردة من الدول الأعضاء تؤيد النظر في مشاريع التوصيات الجديدة هذه بغرض الموافقة عليها في اجتماع لجنة الدراسات، عندئذ سوف تُكرَّس جلسة عامة **في 26 أبريل 2013** لتطبيق إجراءات الموافقة.

ولذلك فإنني أدعو إدارتكم إلى إيفاد ممثل إلى الاجتماع. **ويرجى من إدارات الدول الأعضاء في الاتحاد** بيان اسم رئيس وفدها. وإذا كانت إدارتكم ترغب في أن يمثلها في الاجتماع وكالة تشغيل معتمدة أو منظمة علمية أو صناعية أو أي كيان آخر يتعامل في مسائل الاتصالات، ينبغي إبلاغ المدير بذلك طبقاً لأحكام الرقم 239 من المادة 19 من اتفاقية الاتحاد.

6 ويمكن الاطلاع على جدول الأعمال وجميع المعلومات ذات الصلة فيما يتعلق باجتماع لجنة الدراسات 17 في الرسالة الجماعية التي ستصدر مستقبلاً.

7 وفي أعقاب الاجتماع سوف يعلن مدير مكتب تقييس الاتصالات، في رسالة معممة، عن القرار المُتَخّذ بشأن هذه التوصيات. ولسوف تُنشر هذه المعلومات أيضاً في النشرة التشغيلية للاتحاد.

وتفضلوا بقبول فائق التقدير والاحترام.

مالكولم جونسون
مدير مكتب تقييس الاتصالات

**الملحقات:** **1**

**الملحـق 1
(بالرسالة المعممة 311 لمكتب تقييس الاتصالات)**

ملخص نصوص التوصيات والوثائق التي ترد فيها

مشروع التوصية الجديدة ITU‑T X. 1126 (X.msec-6)، جوانب الأمن في الهواتف الذكية
الوثيقة COM 17 ‑ R 67

ملخص

في ظل التطور المستمر للخصائص الوظيفية وتوسع التطبيقات، تواجه الهواتف الذكية العديد من التهديدات الأمنية التي يمكن أن تسبب مشاكل خطيرة على الصعيد الاجتماعي والاقتصادي. وتتمثل أهداف التوصية ITU-T X.1126 في حماية الخصوصية الشخصية للمستخدمين، وتحسين أمن المعلومات في الهواتف الذكية.

وتحدد هذه التوصية التهديدات التي تتعرض لها الهواتف الذكية والتي تصنف في فئتين هما نقاط الضعف والهجمات. ولتلبية أهداف الأمن هذه، توصّف هذه التوصية إطاراً أمنياً تراتبياً ومتطلبات الأمن ذات الصلة للهواتف الذكية. وفيما يتعلق بالإطار الأمني، تقدم هذه التوصية الحلول الأمنية اللازمة من خلال تحسينات للأنظمة وأدوات أمنية.

مشروع التوصية الجديدة ITU-T X.1154 (X.sap-4)، الإطار العام للاستيقان المجمع في بيئات يتعدد فيها مقدمو خدمة الهوية
الوثيقة COM 17 ‑ R 68

ملخص

في الآونة الأخيرة، تفاقمت سرقات الهوية، فصار العديد من خدمات التطبيقات، والخدمات المالية بشكل خاص، يتطلب أساليب استيقان أكثر موثوقية أو مجمعة، كالاستيقان متعدد العوامل. فعلى سبيل المثال، يُستخدم استيقان بكلمة مرور لمرة واحدة وغيره من أساليب الاستيقان الجديدة بدلاً من الاستيقان التقليدي القائم على كلمة المرور.

وتوفر توليفات من أساليب الاستيقان لمقدمي خدمة الهوية (IdSP) المتعددين القدرة على تعزيز ضمان الاستيقان. وتوفر التوصية ITU-T X.1154 الإطار العام للاستيقان المجمع في بيئات يتعدد فيها مقدمو خدمة الهوية إلى مقدم خدمة. وفي هذه التوصية، يُنظر في ثلاثة أنواع من أساليب الاستيقان المجمع: الاستيقان متعدد العوامل، والاستيقان متعدد الأساليب والاستيقانات المتعددة.

ويصف الإطار الوارد في هذه التوصية النماذج والعمليات الأساسية والمتطلبات الأمنية لكل مكون من مكونات أي نموذج وكل رسالة بين مكونات النموذج للحفاظ على مستوى عام من ضمان الاستيقان في حالات الجمع بين مقدمي خدمة هوية متعددين.

وبالإضافة إلى ذلك، يصف الإطار أيضاً النماذج والعمليات الأساسية والمتطلبات الأمنية لدعم خدمة الاستيقان التي تدير توليفة من مقدمي خدمة هوية متعددين.

مشروع التوصية الجديدة ITU-T X.1526 (X.oval)، اللغة المفتوحة لنقاط الضعف والتقييم
الوثيقة COM 17 ‑ R 64

ملخص

تتناول هذه التوصية استخدام اللغة المفتوحة لنقاط الضعف والتقييم (OVAL). وهذه اللغة هي معيار دولي لأمن المعلومات يُعرف في مجتمع أمن المعلومات، ينهض بمحتوى أمني مفتوح ومتاح للجمهور، ويقيّس نقل هذه المعلومات عبر كل أنواع أدوات الأمن وخدماته. وتتضمن لغة OVAL لغةً تُستخدم لتشفير تفاصيل النظام ومجموعة متنوعة من مستودعات المحتويات القائمة في جميع أنحاء مجتمع أمن المعلومات. وتقيّس اللغة الخطوات الرئيسية الثلاث لعملية التقييم، وهي: تمثيل معلومات تشكيل الأنظمة، لأغراض الاختبار؛ وتحليل النظام بحثاً عن وجود حالة موصَّفة للآلة (نقطة ضعف، أو تشكيل، أو حالة رقعة برمجية، وما إلى ذلك)؛ والإبلاغ عن نتائج هذا التقييم. أما المستودعات فهي مجموعات من المحتويات المفتوحة والمتاحة للجمهور تستخدم هذه اللغة.

وقد وضع مجتمع OVAL ثلاثة مخططات مكتوبة بلغة الوسم القابلة للتوسيع (XML) لتكون بمثابة إطار ومفردات للغة OVAL. وتقابل هذه المخططات الخطوات الثلاث لعملية التقييم: مخطط خصائص نظام OVAL لتمثيل معلومات النظام، ومخطط تعريف OVAL للتعبير عن حالة محددة للآلة، ومخطط نتائج OVAL للإبلاغ عن نتائج تقييم.

ويقع المحتوى المكتوب بلغة OVAL في واحد من العديد من المستودعات الموجودة داخل مجتمع أمن المعلومات. ويُعرف أحد هذه المستودعات بمستودع OVAL. وذلك هو مكان الاجتماع المركزي لمجتمع OVAL لمناقشة تعاريف OVAL وتحليلها وتخزينها ونشرها. ويحدد كل تعريف في مستودع OVAL ما إذا كانت توجد نقاط ضعف برمجية أو مشكلة تشكيل أو برنامج أو رقعة برمجية في أي نظام.

ويسهم مجتمع أمن المعلومات في تطوير لغة OVAL من خلال المشاركة في إنشاء هذه اللغة OVAL في منتدى مطوري اللغة OVAL، وبكتابة تعاريف لمستودع OVAL من خلال منتدى مجتمع OVAL. وهناك مجلس للغة OVAL يتألف من ممثلين من طيف واسع من دوائر الصناعة والهيئات الأكاديمية والمنظمات الحكومية من مختلف أنحاء العالم، وهي تشرف على لغة OVAL وتقرها وتراقب نشر التعاريف في الموقع الإلكتروني لهذه اللغة. وهذا يعني أن لغة OVAL تعبر عن رؤى ومجموع خبرات أوسع مجموعة ممكنة من المهنيين العاملين في إدارة الأمن والأنظمة في جميع أنحاء العالم.

مشروع التوصية الجديدة ITU-T X.1544 (X.capec)، تعداد أنماط الهجوم الشائعة وتصنيفها
الوثيقة COM 17 ‑ R 65

ملخص

إن التوصية بشأن تعداد أنماط الهجوم الشائعة وتصنيفها (CAPEC) هي مواصفة قائمة على لغتي XML/XSD للتعرف على أنماط الهجوم ووصفها وتعدادها. وتعد أنماط الهجوم 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 الهجوم الشائعة وتصنيفها (CAPEC) إلى توفير كتيب إرشادي لأنماط الهجوم يتاح للجمهور إلى جانب مخطط شامل ومنهجية تصنيف.

ويتيح تعداد أنماط الهجوم الشائعة وتصنيفها (CAPEC) ما يلي:

• تقييس التقاط ووصف أنماط الهجوم؛

• جمع أنماط الهجوم المعروفة في تعداد متكامل يمكن أن يستفيد منه مجتمع أمن المعلومات باستمرار وعلى نحو فعّال؛

• تصنيف أنماط الهجوم بحيث يسهل على المستخدمين تحديد مجموعة فرعية تتناسب مع سياقهم من كامل التعداد؛

• ربط أنماط الهجوم بنقاط الضعف (CWE) التي تكون فعالة تجاهها من خلال إحالات صريحة.

ويستفيد مجتمع CAPEC والأطراف المعنية الأخرى من أكبر عدد ممكن من المصادر والأمثلة لوضع تعاريف محددة وموجزة لعناصر قاموس CAPEC ومجموعة متنوعة من الآراء وهياكل شجرة التصنيف.

\_\_\_\_\_\_\_\_\_\_\_\_