|  |  |
| --- | --- |
| **Oficina de Normalizaciónde las Telecomunicaciones** | **logo_S_** |
|  |  |

 Ginebra, 27 de septiembre de 2012

|  |  |  |
| --- | --- | --- |
| Ref.:Tel.:Fax: | **Circular TSB 311**COM 17/MEU+41 22 730 5866+41 22 730 5853 | - A las Administraciones de los Estados Miembros de la Unión |
| Correo-e: | tsbsg17@itu.int  | **Copia**:- A los Miembros del Sector UIT‑T;- A los Asociados del UIT‑T;- A las Instituciones Académicas del UIT-T;- Al Presidente y a los Vicepresidentes de laComisión de Estudio 17;- Al Director de la Oficina de Desarrollo de las Telecomunicaciones;- Al Director de la Oficina de Radiocomunicaciones |

|  |  |
| --- | --- |
| Asunto: | **Reunión de la Comisión de Estudio 17 para la aprobación de los proyectos de nueva Recomendación UIT-T X.1126, X.1154, X.1526 y X.1544****de conformidad con las disposiciones de la Resolución 1, Sección 9, de la AMNT (Johannesburgo, 2008)Ginebra, 26 de abril de 2013** |

Muy Señora mía/Muy Señor mío:

1 A petición del Presidente de la Comisión de Estudio 17, *Seguridad*, tengo el honor de informarle que esta Comisión de Estudio, que se reunirá del 17 al 26 de abril de 2013, se propone aplicar el procedimiento descrito en la Resolución 1, Sección 9, de la AMNT (Johannesburgo, 2008) para la aprobación de los mencionados proyectos de nueva Recomendación.

2 El **anexo 1** contiene el título y el resumen de los proyectos de nueva Recomendación UIT‑T, con indicación de los documentos en que figuran.

3 Todo Estado Miembro, Miembro de Sector, Asociado o Institución Académica de la UIT consciente de la titularidad de una patente propia o ajena que pueda cubrir total o parcialmente los proyectos de Recomendación propuestos para aprobación debe poner esa información en conocimiento de la TSB, de conformidad con la política sobre patentes del UIT‑T/UIT-R/ISO/CEI.

Puede accederse en línea a la información disponible sobre patentes a través de la dirección Web del UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Teniendo en cuenta las disposiciones de la Resolución 1, Sección 9, le agradecería que me comunicase **antes** de las 24.00 horas UTC **del 5 de abril de 2013** si su Administración otorga a la Comisión de Estudio 17 la autoridad necesaria para que durante su reunión puedan considerar la aprobación de estos proyectos de nueva Recomendación.

Si algunos Estados Miembros opinan que no puede procederse a considerar la aprobación, deben indicar sus razones de desaprobación así como los posibles cambios que facilitarían el nuevo examen y la aprobación de los proyectos de nueva Recomendación.

5 Si el 70% como mínimo de las respuestas de los Estados Miembros están a favor de que se considere la aprobación de estos proyectos de nueva Recomendación en la reunión de la Comisión de Estudio, **el 26 de abril de 2013** se dedicará una Sesión Plenaria a la aplicación del procedimiento de aprobación.

Invito pues a su Administración a que envíe un representante a dicha reunión. Se invita a las **Administraciones de los Estados Miembros de la Unión** a precisar el nombre de su Jefe de delegación. Si su Administración desea estar representada en esa reunión por una empresa de explotación reconocida, un organismo científico o industrial u otra entidad que se ocupe de cuestiones de telecomunicaciones, habrá de comunicarlo al Director de conformidad con lo dispuesto en el Artículo 19, número 239, del Convenio de la UIT.

6 El orden del día y toda la información pertinente sobre la reunión de la Comisión de Estudio 17 figurarán en una carta colectiva que se publicará en el futuro.

7 Después de la reunión, el Director de la TSB notificará por circular la decisión tomada sobre estas Recomendaciones. Esta información se publicará también en el Boletín de Explotación de la UIT.

Le saluda atentamente.

Malcolm Johnson
Director de la Oficina de
Normalización de las Telecomunicaciones

**Anexo: 1**

**ANEXO 1**

**(a la Circular TSB 311)**

Resumen y ubicación de los textos

Proyecto de nueva Recomendación UIT-T X.1126 (X.msec-6), Aspectos de seguridad de los teléfonos inteligentes ("smartphones")
COM17-R67

Resumen

Debido al continuo desarrollo de las funcionalidades y la expansión de las aplicaciones, los teléfonos inteligentes ("smartphones") se enfrentan a muchas amenazas contra la seguridad que pueden causar importantes problemas sociales y económicos. Los objetivos de la Recomendación UIT-T X.1126 son la protección de la privacidad personal de los usuarios y la mejora de la seguridad en la información de los "smartphones".

Esta Recomendación identifica las amenazas a los "smartphones" clasificadas en vulnerabilidades y ataques. Para satisfacer estos objetivos de seguridad, la Recomendación especifica un marco de seguridad jerárquico y los requisitos de seguridad pertinentes para los "smartphones". Con respecto al marco de seguridad, la Recomendación proporciona las soluciones de seguridad necesarias mediante mejoras en el sistema y herramientas de seguridad.

Proyecto de nueva Recomendación UIT-T X.1154 (X.sap-4), Marco general de autentificación combinada en múltiples entornos de proveedor de servicio de identidad
COM17-R68

Resumen

Recientemente, muchos servicios de aplicaciones, especialmente los servicios financieros, requieren métodos de autentificación más fiables o combinados tales como la autentificación multifactorial, debido al número cada vez mayor de robos de identidad (ID). Por ejemplo, en vez de los sistemas de autentificación tradicionales basados en una palabra clave se emplea autentificación con contraseña volátil y otros nuevos métodos de autentificación.

Las combinaciones de métodos de autentificación proporcionan a múltiples proveedores de servicio de identidad (IdSP) la posibilidad de mejorar la garantía de la autentificación. La Recomendación UIT-T X.1154 presenta el marco general de autentificación combinada en múltiples entornos IdSP para un proveedor de servicio. En esta Recomendación se consideran tres tipos de métodos de autentificación combinada: autentificación multifactorial, autentificación multimétodo y autentificaciones múltiples.

El marco de esta Recomendación describe modelos, operaciones básicas y requisitos de seguridad para cada componente del modelo y cada mensaje entre los componentes del modelo a fin de mantener un nivel global de garantía de la autentificación en situaciones de una combinación de múltiples IdSP.

Además, el marco también describe modelos, operaciones básicas y requisitos de seguridad para soportar el servicio de autentificación que gestiona una combinación de múltiples IdSP.

Proyecto de nueva Recomendación UIT-T X.1526 (X.oval), Vulnerabilidad abierta y lenguaje de evaluación
COM17-R64

Resumen

Esta Recomendación sobre la utilización de la vulnerabilidad abierta y el lenguaje de evaluación (OVAL), que es una norma internacional, de seguridad de la información y comunitaria que promueve un contenido de seguridad abierto y públicamente disponible y normaliza la transferencia de esta información a través de todo el espectro de herramientas y servicios de seguridad. OVAL incluye un lenguaje utilizado para codificar los detalles del sistema y una serie de depósitos de contenido a través de toda la comunidad. El lenguaje normaliza los tres pasos principales del proceso de evaluación: representando la información de configuración de los sistemas para la prueba, analizando el sistema para detectar la presencia del estado de máquina especificado (vulnerabilidad, configuración, estado parche, etc.), e informando sobre los resultados de esta evaluación. Los depósitos son colecciones de contenido abierto y públicamente disponible que utiliza el lenguaje.

La comunidad OVAL ha desarrollados tres esquemas escritos en lenguaje de marcaje extensible (XML) que sirve de marco y vocabulario del lenguaje OVAL. Estos esquemas corresponden a los tres pasos del proceso de evaluación: un esquema de las características del sistema OVAL para representar la información del sistema, un esquema de definición de OVAL para expresar un estado de máquina específico y un esquema de resultados OVAL para informar sobre los resultados de la evaluación.

El contenido escrito del lenguaje OVAL esta ubicado en uno de los muchos depósitos que se encuentran en la comunidad. Uno de esos depósitos se conoce con el nombre de Depósito OVAL. Se trata del lugar de reunión central para que la comunidad OVAL discuta, analice, almacene y difunda las definiciones OVAL. Cada definición en el Deposito OVAL determina si está presente en un sistema una vulnerabilidad de software especificada, un problema de configuración, un programa o un parche.

La comunidad de seguridad de la información contribuye al desarrollo de OVAL participando en la creación del lenguaje OVAL en el Foro de Creadores de OVAL y escribiendo definiciones para el Depósito OVAL a través del Foro de Comunidad OVAL. Una Junta OVAL, compuesta por representantes de un amplio espectro de la industria, las instituciones académicas y las organizaciones gubernamentales de todo el mundo, supervisa y aprueba el lenguaje OVAL y controla la difusión de las definiciones contenidas en la dirección web de OVAL. Ello significa que OVAL refleja el conocimiento y la experiencia combinada del conjunto más amplio posible de profesionales de la administración de la seguridad y los sistemas de todo el mundo.

Proyecto de nueva Recomendación UIT-T X.1544 (X.capec), Enumeración y clasificación de pautas de ataques comunes
COM17-R65

Resumen

La Recomendación sobre enumeración y clasificación de pautas de ataque comunes (CAPEC) es una especificación basada en XML/XSD para la identificación, descripción y enumeración de las pautas de ataque, que constituyen un poderoso mecanismo para capturar y comunicar la perspectiva del atacante. Se trata de descripciones de métodos comunes para exportar el software. Se derivan del concepto de pautas de diseño aplicadas en un contexto destructivo en vez de constructivo y se generan a partir de un profundo análisis de ejemplos de explotación específicos del mundo real. El objetivo de CAPEC es proporcionar un catálogo públicamente disponible de pautas de ataque junto con un esquema completo y una taxonomía de clasificación.

CAPEC permite:

• Normalizar la captura y descripción de las pautas de ataque.

• Recopilar pautas de ataque conocidas en una enumeración integrada que puede ser compensada por la comunidad de una manera coherente y efectiva.

• Clasificar las pautas de ataque de forma que los usuarios puedan identificar fácilmente el subconjunto de toda la enumeración apropiado para su contexto.

• Vincular las pautas de ataque y la debilidades (CWE) eficaces a través de referencias especificas.

La comunidad CAPEC y otras partes interesadas recopilan el mayor número de fuentes y ejemplos posible para desarrollar las definiciones específicas y sucintas de los elementos del Diccionario CAPEC y una variedad de opiniones y clasificaciones con estructura de árbol.

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