Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1524

(03/2012)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Intercambio de información de ciberseguridad – Intercambio de estados/vulnerabilidad

Lista de puntos débiles comunes

Recomendación UIT-T X.1524

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	**X.1520–X.1539**
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1524

Lista de puntos débiles comunes

Resumen

En la presente Recomendación sobre la utilización de la Lista de puntos débiles comunes (*common weakness enumeration* o CWE) se describe un mecanismo estructurado para el intercambio de datos sobre puntos débiles de la seguridad de la información que pone nombres comunes a problemas ampliamente conocidos en el ámbito del software comercial o de fuente abierta utilizado en las redes de comunicaciones, en dispositivos de usuario o en otras tecnologías de la información y las comunicaciones (TIC) capaces de ejecutar programas informáticos. La CWE permite analizar, describir, seleccionar y utilizar más eficazmente las herramientas y servicios de seguridad del software que pueden detectar dichas debilidades en códigos fuente y sistemas operativos, así como comprender y gestionar mejor las deficiencias presentes en la arquitectura y el diseño del software. En la presente Recomendación se define la utilización de la CWE como un mecanismo para poder utilizar conjuntamente herramientas, servicios y bases de conocimientos sobre seguridad del software y otras capacidades, así como para comparar mejor las herramientas y servicios de seguridad. La CWE ofrece asimismo información contextual acerca de los posibles riesgos, consecuencias, soluciones y detalles técnicos relativos a las repercusiones que los puntos débiles del software podrían entrañar para un sistema informático.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1524	2012-03-02	17

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en esta Recomendación 1
4 Abreviaturas y acrónimos 3
5 Convenios 3
6 Requisitos de alto nivel 3
7 Exactitud 5
8 Eficacia 5
9 Documentación 6
10 Versión de la CWE utilizada 6
11 Revocación de la compatibilidad CWE 6
12 Autoridad de revisión 7
Anexo A – Requisitos específicos de los tipos de capacidades 8
A.2 Requisitos de las herramientas 8
A.3 Requisitos de los servicios de seguridad 9
A.4 Requisitos de las capacidades en línea 10
Anexo B – Requisitos de los medios 11
B.3 Documentos electrónicos (HTML, procesador de texto, PDF, texto ASCII, etc.) 11
B.4 Interfaz gráfica de usuario (GUI) 11
Apéndice I – Lista de repositorios CWE para identificadores e información contextual conexa 12
Apéndice II – Lista de autoridades de revisión 13
Bibliografia 14

Introducción

En la presente Recomendación sobre la Lista de puntos débiles comunes (CWE) se describe el uso de la CWE como un medio estructurado para el intercambio de conjuntos de datos mensurables y unificados sobre puntos débiles del software a fin de poner nombres comunes a problemas ampliamente conocidos. La CWE permite asimismo analizar, describir, seleccionar y utilizar más eficazmente las herramientas y servicios de seguridad del software capaces de detectar dichas debilidades en códigos fuente y sistemas operativos, así como comprender y gestionar mejor las deficiencias presentes en la arquitectura y el diseño del software.

La CWE pretende adoptar una perspectiva global con respecto a las causas que se ocultan tras todos los puntos débiles y fallos ampliamente conocidos, ya procedan de la arquitectura, el diseño, el código o la implementación del software. Aunque la CWE se ha concebido para contener información consolidada, su principal objetivo es identificar los puntos débiles que pueden causar vulnerabilidades y riesgos. La autoridad de revisión será la encargada de determinar la conformidad de la utilización de los identificadores CWE con arreglo a la presente Recomendación.

La CWE se basa en trabajos realizados por la comunidad de ciberseguridad, tales como el gran número de vulnerabilidades reales especificadas en la Recomendación UIT-T X.1520 – Vulnerabilidades y exposiciones comunes (*common vulnerabilities and exposures* o CVE). Se ha recurrido a numerosas fuentes y ejemplos con el objetivo de elaborar definiciones específicas y sucintas relativas a los elementos que componen la CWE y sus estructuras de clasificación en árbol. Del mismo modo, se han establecido las correspondencias adecuadas entre las CWE y los nombres de las CVE a fin de que a cada identificador CWE se le asigne una lista de nombres CVE específicos que pertenezca a dicha categoría concreta de CWE. Para la elaboración de la lista y las clasificaciones en árbol de los puntos débiles comunes del software, se pretende aplicar un enfoque lo más integral posible que abarque los dominios conceptuales, técnicos y de negocio pertinentes.

La Recomendación UIT-T X.1524 sobre la Lista de puntos débiles comunes (CWE) ha sido elaborada en colaboración con The MITRE Corporation teniendo en cuenta la importancia de mantener, en la medida de lo posible, la compatibilidad técnica entre la Recomendación UIT-T X.1524 sobre la Lista de puntos débiles comunes (CWE) y la versión 1.0 del documento "Recomendaciones y requisitos relativos a la compatibilidad CWE y su utilización eficaz" (*Requirements and Recommendations for CWE Compatibility and Effectiveness*), de 28 de julio de 2011, que puede consultarse en la dirección: https://cwe.mitre.org/compatible/requirements_v1.0.html.

Recomendación UIT-T X.1524

Lista de puntos débiles comunes

1 Alcance

En la presente Recomendación sobre la utilización de la Lista de puntos débiles comunes (CWE) se describe un "mecanismo estructurado" para el intercambio global de información sobre los puntos débiles de seguridad presentes en la arquitectura, el diseño, el código o la ejecución del software y que pueden provocar un deterioro en la seguridad, fiabilidad o vulnerabilidad del mismo ante posibles ataques. Existen determinados exámenes de seguridad, servicios de evaluación y herramientas de seguridad capaces de detectar esta clase de puntos débiles del software. Este "mecanismo estructurado" suele denominarse "compatibilidad con la CWE" y define la utilización correcta de la CWE. Un punto débil de la seguridad de la información constituye un error del software capaz de entrañar una vulnerabilidad que podría, a su vez, ser utilizada por un pirata informático para acceder a un sistema o una red. Si bien la asignación de identificadores CWE queda fuera del alcance de la presente Recomendación, en el Apéndice I figura una lista de repositorios para identificadores CWE e información contextual conexa.

La CWE, cuya utilización se define en la presente Recomendación, pretende adoptar una perspectiva global con respecto a los errores presentes en la arquitectura, el diseño, el código o la ejecución del software que constituyen las causas raíz de las vulnerabilidades y riesgos del sistema. Aunque la CWE se ha concebido para contener información consolidada, su principal objetivo es identificar, informar y describir dichas causas raíz con el fin de que los diseñadores puedan evitarlas, los equipos de desarrollo las comprueben y gestionen, y las herramientas y servicios de seguridad del sistema las notifiquen correctamente.

La Recomendación UIT-T X.1524 sobre la Lista de puntos débiles comunes (CWE) ha sido elaborada en colaboración con The MITRE Corporation teniendo en cuenta la importancia de mantener, en la medida de lo posible, la compatibilidad técnica entre la Recomendación UIT-T X.1524 sobre la Lista de puntos débiles comunes (CWE) y la versión 1.0 del documento "Recomendaciones y requisitos relativos a la compatibilidad con la CWE y su utilización eficaz" (*Requirements and Recommendations for CWE Compatibility and Effectiveness*), de 28 de julio de 2011, que puede consultarse en la dirección https://cwe.mitre.org/compatible/requirements.html.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 porcentaje de exactitud: Porcentaje de elementos de seguridad de la muestra de revisión que hacen referencia a los identificadores de la CWE correctos.

3.2.2 capacidad: Herramienta de evaluación, entorno de desarrollo integrado (IDE), herramienta de revisión de código, compilador de verificación de código, base de datos, sitio web, advertencia o servicio que facilita información sobre los puntos débiles presentes en la implementación, el diseño

o la arquitectura del software y que pueden dar lugar a una posible vulnerabilidad en la seguridad del software.

3.2.3 formulario de evaluación de los requisitos de compatibilidad con la CWE: Este formulario de evaluación contiene una serie de preguntas dirigidas a solicitar al propietario de la capacidad que documente la conformidad de la misma con los requisitos de compatibilidad descritos en la presente Recomendación (compatibilidad CWE) y relativos a los textos, imágenes o páginas web de referencia, así como instrucciones acerca de dónde enviar el formulario una vez cumplimentado o cómo solicitar a la autoridad de revisión aclaraciones sobre el procedimiento para completar dicho formulario.

3.2.4 formulario de evaluación de los requisitos de eficacia CWE: Este formulario de evaluación contiene una serie de preguntas dirigidas a solicitar al propietario de la capacidad que documente la conformidad de la misma con los requisitos de eficacia descritos en la presente Recomendación y relativos a los textos, imágenes o páginas web de referencia, así como instrucciones acerca de dónde enviar el formulario cumplimentado y las pruebas requeridas, o cómo solicitar a la autoridad de revisión aclaraciones sobre el procedimiento para completar dicho formulario.

3.2.5 prueba de eficacia: Proceso que determina si una capacidad utiliza eficazmente la CWE.

3.2.6 mapa/correspondencia: Especificación de las relaciones entre los puntos débiles contenidos en un repositorio y los elementos de la CWE relacionados con dichos puntos débiles.

3.2.7 propietario: Custodio (persona física o jurídica) responsable de la capacidad.

3.2.8 repositorio: Conjunto implícito o explícito de datos sobre puntos débiles del software relacionados con la seguridad que sustenta una capacidad, por ejemplo, una base de datos sobre puntos débiles, el conjunto de patrones de un analizador de código o un sitio web.

3.2.9 revisión: Proceso para determinar si una capacidad es compatible con la CWE.

3.2.10 autoridad de revisión: Toda entidad que realice una revisión o una prueba de eficacia y esté autorizada para conceder la condición de compatible con la CWE o determinar si la CWE se está utilizando de manera eficaz.

NOTA – En el Apéndice II figura una lista de las autoridades de revisión.

3.2.11 versión de revisión: Versión fechada de la CWE que se utiliza para determinar la compatibilidad con la CWE de una capacidad o si ésta la utiliza de manera eficaz.

3.2.12 elemento de seguridad: Registro de base de datos, sonda de evaluación, firma, etc., relacionada con un punto débil de seguridad específico.

3.2.13 tarea: Sonda, verificación, firma u otro elemento de una herramienta que realiza una acción que genera información de seguridad (es decir, el elemento de seguridad).

3.2.14 resultados de la prueba: Datos que reflejan la conclusión de la prueba de eficacia.

3.2.15 herramienta: Aplicación de software o dispositivo que examina una parte del software, un código binario, etc., y produce información sobre los puntos débiles de seguridad. Por ejemplo, un analizador de seguridad del código fuente, una herramienta de evaluación de la calidad del código, un compilador de verificación de código o un entorno de desarrollo.

3.2.16 usuario: Consumidor o posible consumidor de la capacidad.

3.2.17 vulnerabilidad: Punto débil del software que puede utilizarse para acceder a un sistema o a la información que contiene (con arreglo a la Recomendación UIT-T X.1500).

3.2.18 punto débil: Error o imperfección presente en el código, el diseño, la arquitectura o la ejecución del software que puede, en un momento dado, convertirse en una vulnerabilidad o favorecer la aparición de otras vulnerabilidades.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ASCII Código normalizado estadounidense para el intercambio de información (*american standard code for information interchange)*

CCR Representación de reclamaciones de cobertura (*coverage claim representation*)

CGI Interfaz de pasarela común (*common gateway interface*)

CWE Lista de puntos débiles comunes (*common weakness enumeration)*

GUI Interfaz gráfica de usuario (*graphical user interface)*

HTML Lenguaje de marcación de hipertexto (*hypertext markup language)*

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol)*

TIC Tecnologías de la información y la comunicación

PDF Formato de documento portable (*portable document format)*

POC Persona de contacto (*point of contact)*

URL Localizador uniforme de recursos (*uniform resource locator)*

XML Lenguaje de etiquetado extensible (*extensible markup language)*

5 Convenios

Ninguno.

6 Requisitos de alto nivel

A continuación se definen los conceptos, funciones y responsabilidades relacionados con la utilización adecuada de los identificadores CWE para el intercambio datos entre distintas capacidades de puntos débiles de seguridad (herramientas, repositorios y servicios) de forma que dichas capacidades puedan utilizarse conjuntamente y se facilite la comparación entre herramientas y servicios de puntos débiles de seguridad.

6.1 El propietario de la capacidad deberá ser una entidad jurídica válida, es decir, una organización o una persona con un número de teléfono, dirección de correo electrónico y dirección postal válidos.

6.2 La capacidad aportará un valor o una información adicional, además de los que facilita la propia CWE (es decir, nombre, descripción, riesgos, referencias e información conexa sobre el punto débil).

6.3 El propietario de la capacidad facilitará a la autoridad de revisión una persona de contacto técnico cualificada para responder a las dudas sobre la exactitud de la correspondencia y las funcionalidades de la capacidad relacionadas con la CWE, así como para coordinar las pruebas a las que se someterá la capacidad en aras de evaluar su eficacia a la hora de identificar las CWE.

6.4 La capacidad estará a disposición pública, o de un conjunto de consumidores, en una versión pública o de producción, ya sea a través de una página web de uso general, en forma de código abierto, poniéndola a la venta o como servicio disponible por contrato.

6.5 Para la compatibilidad con la CWE, el propietario de la capacidad presentará a la autoridad de revisión un "Formulario de evaluación de los requisitos de compatibilidad CWE" cumplimentado.

6.6 El propietario de la capacidad dará a la autoridad de revisión acceso libre al repositorio de la capacidad a fin de que ésta pueda determinar si satisface los requisitos de exactitud de correspondencia conexos.

6.7 El propietario de la capacidad autorizará a la autoridad de revisión a utilizar el repositorio con el objetivo de identificar todo punto débil que deba añadirse a la CWE.

6.8 Para que una capacidad cumpla con el requisito de eficacia CWE, deberá cumplir el requisito de compatibilidad CWE.

6.9 Para que una capacidad cumpla con el requisito de eficacia CWE, el propietario de la misma presentará a la autoridad de revisión un "Formulario de evaluación de los requisitos de eficacia CWE" cumplimentado.

6.10 Para que una capacidad cumpla con los requisitos de eficacia CWE, el propietario de la misma presentará a la autoridad de revisión los resultados de las pruebas de eficacia adjuntos al "Formulario de evaluación de los requisitos de eficacia CWE" a fin de que ésta pueda determinar si la capacidad satisface todos los requisitos de eficacia conexos.

6.11 El propietario de la capacidad acordará respetar todos los requisitos de compatibilidad y de eficacia CWE obligatorios entre los que se incluyen los requisitos obligatorios aplicables al tipo específico de capacidad en cuestión.

6.12 Para la compatibilidad CWE, la capacidad autorizará a los usuarios a localizar los elementos de seguridad utilizando los identificadores CWE ("búsqueda por CWE").

6.13 Para la compatibilidad CWE, cuando la capacidad presente elementos de seguridad al usuario, permitirá que éste obtenga los identificadores CWE asociados ("resultado de la CWE").

6.14 Para la compatibilidad CWE, la correspondencia de la capacidad deberá vincular con precisión los elementos de seguridad y los identificadores CWE correspondientes ("exactitud de la correspondencia").

6.15 Para la compatibilidad CWE, la documentación de la capacidad deberá describir adecuadamente la CWE, la compatibilidad CWE y cómo utiliza la capacidad las funcionalidades relacionadas con la CWE ("documentación de la CWE").

6.16 Para la compatibilidad CWE, la documentación pública de la capacidad enumerará explícitamente los identificadores CWE que el propietario de la misma considera que abarca como parte de su funcionalidad ("cobertura CWE").

6.17 Para la compatibilidad CWE, el sitio web público de la capacidad debería facilitar la cobertura CWE de la capacidad en forma de documentos XML de representación de reclamaciones de cobertura (CCR) de la CWE.

6.18 Para que una capacidad cumpla los requisitos de la eficacia CWE, los resultados obtenidos por dicha capacidad en las pruebas de evaluación de los identificadores CWE (incluidos en la cobertura CWE) se publicarán en el sitio web de la autoridad de revisión de la CWE ("resultados de las pruebas CWE").

6.19 La capacidad indicará la fecha de la versión CWE utilizada ("versión utilizada").

6.20 La capacidad cumplirá los requisitos adicionales establecidos para su categoría específica recogidos en el Anexo A.

6.21 La capacidad satisfará todos los requisitos de su medio de distribución, según se especifica en el Anexo B.

6.22 No se requiere que la capacidad cumpla las siguientes funciones:

- utilizar las mismas descripciones o referencias que la CWE;
- incluir todos los identificadores CWE en su repositorio.

6.23 Si la capacidad no satisface todos los requisitos aplicables indicados anteriormente (6.1 a 6.22), el propietario de la capacidad no anunciará que la misma se ajusta a los requisitos de compatibilidad CWE o de eficacia CWE descritos en la presente Recomendación.

7 Exactitud

La compatibilidad CWE sólo facilita el intercambio de datos y su correlación si la correspondencia de la capacidad es exacta. Por tanto, las capacidades compatibles CWE deben satisfacer los requisitos mínimos de exactitud que se enumeran a continuación.

7.1 El repositorio presentará una exactitud del 100%.

7.2 Durante el periodo de revisión, el propietario corregirá cualquier error de correspondencia detectado por la autoridad de revisión.

7.3 Después del periodo de revisión, el propietario debería corregir cualquier error de correspondencia identificado en un periodo de tiempo razonable desde que informó del mismo, a saber, en las siguientes dos (2) versiones del repositorio de la capacidad o en seis (6) meses, escogiéndose entre ambos el periodo más corto.

7.4 El propietario de la capacidad deberá preparar y firmar una declaración en la que afirme que, en su conocimiento como propietario de la capacidad, no existen errores de correspondencia.

7.5 Si la capacidad se basa en otra capacidad compatible con la CWE o la utiliza (en adelante, capacidad "fuente"), y el propietario de la misma descubre que la capacidad fuente presenta errores de correspondencia, deberá informar de tales errores al propietario de la capacidad fuente.

8 Eficacia

El concepto de eficacia hace referencia a que una capacidad presenta una transparencia tal de su funcionamiento, que permite a los posibles usuarios de la misma identificar los correspondientes puntos débiles del software. Este conocimiento sobre las posibilidades que tiene la capacidad de detectar puntos débiles en distintos niveles de complejidad resulta interesante para los usuarios a la hora de decidir si utilizar una capacidad o confiar en los resultados obtenidos por otros con la misma. Por consiguiente, las capacidades que se consideren eficaces en términos de la CWE han de cumplir los siguientes requisitos de eficacia mínimos.

8.1 En el apartado correspondiente del "Formulario de evaluación de los requisitos de eficacia CWE", el propietario de la capacidad declarará qué identificadores CWE permiten considerar que la capacidad es eficaz en la localización de puntos débiles. Para ello, puede utilizarse uno o varios documentos XML de representación de declaración de cobertura (CCR) CWE.

8.2 Para los identificadores CWE declarados, el propietario de la capacidad solicitará los conjuntos de pruebas necesarios a fin de utilizar la capacidad para evaluar dichos conjuntos de pruebas relativos a todos los puntos débiles correspondientes a los identificadores CWE declarados.

8.3 Dentro de un plazo de tiempo acordado, el propietario de la capacidad presentará los resultados obtenidos por la misma en la evaluación de los conjuntos de pruebas.

8.4 Los resultados se mostrarán en un fichero para cada conjunto de pruebas evaluado y se identificará el número de la línea donde se ha detectado cada punto débil y junto al identificador CWE adecuado.

8.5 El propietario de la capacidad preparará y firmará una declaración en la que acepte que se publiquen los resultados de las pruebas de dicha capacidad en el sitio web de la CWE.

8.6 El propietario de la capacidad presentará un "Formulario de evaluación de los requisitos de eficacia CWE" revisado junto con una lista actualizada de los identificadores CWE que su capacidad puede localizar eficazmente, con el objeto de poder volver a realizar las pruebas de eficacia para un conjunto de identificadores CWE distinto. Para ello, puede utilizarse uno o varios documentos XML de representación de declaración de cobertura (CCR) CWE actualizados.

9 Documentación

La documentación proporcionada por el propietario de la capacidad junto con la susodicha debe cumplir los requisitos siguientes.

9.1 La documentación incluirá una breve descripción de la CWE y de la compatibilidad CWE, que puede estar basada en extractos literales de documentos del sitio web de la autoridad de revisión de la CWE.

9.2 La documentación describirá cómo puede localizar el usuario elementos de seguridad individuales en el repositorio de la capacidad utilizando los identificadores CWE.

9.3 La documentación describirá cómo puede el usuario obtener identificadores CWE de elementos individuales en el repositorio de la capacidad.

9.4 Si la documentación posee un índice, éste debería incluir referencias a la documentación relativa a la CWE bajo el término "CWE".

10 Versión de la CWE utilizada

Los usuarios deben saber qué versión de la CWE se utiliza en el repositorio de una capacidad en lo que respecta a su correspondencia con la CWE. El propietario de la capacidad puede indicar la vigencia de la correspondencia proporcionando la versión de la CWE o la fecha de la última actualización de la correspondencia.

10.1 La capacidad identificará la versión de la CWE o la fecha de actualización que se utilizó al crear o actualizar la correspondencia en, como mínimo, uno de los siguientes apartados: registros de cambios, listas de nuevas características, ficheros de ayuda u otro mecanismo. La capacidad se considera "actualizada" con respecto a dicha versión o fecha de actualización.

10.2 Cada nueva versión de la capacidad debería estar actualizada con relación a la versión de la CWE publicada no más de cuatro (4) meses antes de que dicha capacidad se pusiera a disposición de los usuarios. Si una capacidad no satisface este requisito, se considera que está "obsoleta".

10.3 Cuando una nueva versión o actualización de la CWE se ponga a disposición en su página web, el propietario de la capacidad habrá de comunicar a los usuarios actuales y futuros cuándo actualizará el repositorio de la capacidad.

11 Revocación de la compatibilidad CWE

A continuación se detallan las responsabilidades de la autoridad de revisión con respecto a la revocación de la compatibilidad CWE.

11.1 Si una autoridad de revisión ha verificado que una capacidad cumple los requisitos de compatibilidad CWE o de la eficacia CWE, pero ulteriormente tiene evidencias de que no se cumplen dichos requisitos, la autoridad de revisión puede revocar su aprobación.

11.1.1 La autoridad de revisión identificará los requisitos específicos que no se cumplen.

11.2 La autoridad de revisión determinará si las acciones o reclamaciones del propietario son "deliberadamente equivocadas".

11.2.1 La autoridad de revisión puede interpretar la expresión "deliberadamente equivocadas" como considere oportuno.

11.3 La autoridad de revisión no debería considerar la revocación de la compatibilidad CWE de una misma capacidad en más de una ocasión cada seis (6) meses.

11.4 La autoridad de revisión proporcionará al propietario de la capacidad y a la persona de contacto técnico un aviso de revocación con al menos dos (2) meses de antelación.

11.4.1 Si la autoridad de revisión concluye que las actuaciones o demandas del propietario son deliberadamente equivocadas, puede obviar el periodo de aviso.

11.5 Si el propietario considera que se cumplen los requisitos, puede responder al aviso de revocación proporcionando información que demuestre que la capacidad cumple los requisitos que se han puesto en tela de juicio.

11.6 Si durante el periodo de aviso el propietario modifica la capacidad para que cumpla los requisitos cuestionados, la autoridad de revisión debería desestimar el proceso de revocación de la compatibilidad CWE de dicha capacidad.

11.7 La autoridad de revisión puede retrasar la fecha de revocación.

11.8 La autoridad de revisión publicará la revocación de la compatibilidad CWE o de la eficacia CWE de la capacidad en cuestión en su página web.

11.9 Si la autoridad de revisión concluye que las actuaciones del propietario de la capacidad con respecto a los requisitos de compatibilidad CWE o de eficacia CWE son deliberadamente equivocadas, la revocación debería permanecer en vigor al menos un año.

11.10 La autoridad de revisión puede hacer públicas las razones de la revocación.

11.11 El propietario de la capacidad puede publicar una declaración referente a la revocación en el mismo sitio web.

11.12 Si se revoca la compatibilidad, el propietario de la misma no podrá solicitar una nueva revisión hasta que no termine el periodo de revocación.

12 Autoridad de revisión

12.1 La autoridad de revisión analizará la compatibilidad CWE y la eficacia CWE con respecto a una versión específica de la CWE, a saber, la versión de revisión.

12.2 La autoridad de revisión identificará claramente la versión de revisión utilizada para establecer la compatibilidad o la eficacia de la capacidad.

12.3 La autoridad de revisión identificará claramente la versión del documento de requisitos de compatibilidad y eficacia CWE utilizado para establecer la compatibilidad o la eficacia de la capacidad.

12.4 La autoridad de revisión examinará todos y cada uno de los elementos del repositorio de la capacidad para determinar la exactitud de correspondencia con la CWE.

12.5 La autoridad de revisión debería examinar la exactitud de correspondencia de la capacidad al menos una vez al año.

Anexo A

Requisitos específicos de los tipos de capacidades

(Este anexo forma parte integrante de la presente Recomendación)

Dado que una amplia variedad de capacidades utiliza la CWE, algunas de ellas pueden tener características particulares que precisen una atención especial en lo que respecta a la compatibilidad CWE.

A.1 La capacidad cumplirá todos los requisitos adicionales relacionados con su tipo específico.

A.1.1 Si la capacidad es una herramienta de evaluación, un analizador de la seguridad del código fuente o del código binario, una herramienta de evaluación de la calidad del código, un compilador de verificación del código, un entorno de desarrollo o un producto que integre los resultados de uno o más de los elementos anteriores, satisfará los requisitos de las herramientas, es decir, de A.2.1 a A.2.8.

A.1.2 Si la capacidad es un servicio (por ejemplo, un servicio de evaluación de la seguridad, un servicio de educación o formación, o un servicio de revisión de código y diseño), cumplirá los requisitos de los servicios de seguridad, es decir, de A.3.1 a A.3.5.

A.1.3 Si la capacidad es una base de datos en línea sobre elementos o puntos débiles de seguridad de una aplicación, un recurso web o un sitio de información, satisfará los requisitos de las capacidades en línea, es decir, de A.4.1 a A.4.3.

A.2 Requisitos de las herramientas

A continuación se detallan los requisitos específicos de las herramientas.

A.2.1 La herramienta permitirá al usuario utilizar los identificadores CWE para localizar tareas asociadas en dicha herramienta ("Búsqueda por CWE") proporcionando al menos uno de los mecanismos siguientes: la función "buscar" o "encontrar", la correspondencia entre dichos nombres de tareas de la herramienta y los identificadores CWE, u otro mecanismo que la autoridad de revisión considere suficiente.

A.2.2 Para la elaboración de cualquier informe que identifique elementos de seguridad individuales, la herramienta permitirá al usuario determinar los identificadores CWE asociados a dichos elementos ("Salida por CWE") mediante al menos uno de los siguientes mecanismos: incluir los identificadores CWE directamente en el informe, establecer la correspondencia entre dichos nombres de tareas de la herramienta y los identificadores CWE, u otro mecanismo que la autoridad de revisión considere suficiente.

A.2.3 En la documentación pública se enumerarán explícitamente los identificadores CWE que el propietario de la capacidad considere que la herramienta puede localizar en el software de manera eficaz ("cobertura declarada de compatibilidad CWE").

A.2.4 En el sitio web público de la capacidad se puede publicar la cobertura declarada de compatibilidad CWE en forma de uno o varios documentos XML de representación de declaración de cobertura (CCR) CWE.

A.2.5 Todo informe o correspondencia que sea necesaria satisfará los requisitos de los medios especificados en el Anexo B.

A.2.6 La herramienta, o el propietario de la capacidad, debería proporcionar al usuario una lista con todos los identificadores CWE asociados a las tareas de dicha herramienta.

A.2.7 La herramienta debería permitir al usuario seleccionar un conjunto de tareas a través de un fichero que contenga una lista de identificadores CWE.

A.2.8 La interfaz de la herramienta debería permitir al usuario visualizar, seleccionar y descartar un conjunto de tareas utilizando identificadores CWE individuales.

A.2.9 Si la herramienta no tiene una tarea que esté asociada con un identificador CWE, tal y como se indica en los puntos A.2.5 o A.2.6 sobre requisitos de la herramienta, ésta debería notificar al usuario que no puede realizar la tarea asociada.

A.2.10 El propietario garantizará que: 1) la tasa de falsos positivos es inferior al 100%, es decir, si la herramienta informa sobre la existencia de un elemento de seguridad específico, este dato será correcto al menos una vez; y 2) la tasa de falsos negativos es inferior al 100%, es decir, si tiene lugar un evento negativo relacionado con un elemento de seguridad específico, la herramienta informará de dicho evento al menos una vez.

A.3 Requisitos de los servicios de seguridad

Los servicios de seguridad pueden utilizar en su actividad herramientas relacionadas con la compatibilidad CWE o con la eficacia CWE, pero pueden no ofrecer a sus clientes acceso directo a dichas herramientas. Por tanto, a los clientes les puede resultar difícil identificar y comparar las capacidades de distintos servicios. Los requisitos de los servicios de seguridad abordan esta posible limitación.

A.3.1 El servicio de seguridad deberá poder utilizar los identificadores CWE para indicar al usuario qué elementos de seguridad ha probado, detectado o están cubiertos por la oferta de servicios ("Búsqueda por CWE") mediante uno o más de los siguientes mecanismos: proporcionar al usuario una lista de identificadores CWE que especifiquen los elementos probados, detectados o cubiertos por el servicio; proporcionar al usuario una correspondencia entre los elementos del servicio y los identificadores CWE; responder a una lista de identificadores CWE facilitada por un usuario concretando cuáles han sido probados, detectados o cubiertos por el servicio; o utilizar cualquier otro mecanismo.

A.3.2 Para la elaboración de cualquier informe que identifique elementos de seguridad individuales, el servicio permitirá al usuario determinar los identificadores CWE asociados a dichos elementos ("Salida por CWE") mediante uno o más de los mecanismos siguientes: permitir al usuario incluir identificadores CWE directamente en el informe, proporcionar al usuario la correspondencia entre los elementos de seguridad y los identificadores CWE, o utilizar cualquier otro mecanismo.

A.3.3 En la documentación pública se enumerarán explícitamente los identificadores CWE que el propietario de la capacidad considera que quedan cubiertos de forma eficaz por el servicio de seguridad ("cobertura declarada de compatibilidad CWE").

A.3.4 En el sitio web público de la capacidad se puede publicar la cobertura declarada de compatibilidad CWE en forma de uno o varios documentos XML de representación de declaración de cobertura (CCR) CWE.

A.3.5 Todo informe o correspondencia proporcionada por el usuario satisfará los requisitos de los medios especificados en el Anexo B.

A.3.6 Si el servicio proporciona al usuario acceso directo a un producto que identifique elementos de seguridad, el producto debería ser compatible y eficaz en relación con la CWE.

A.3.7 El propietario garantizará que: 1) la tasa de falsos positivos es inferior al 100%, es decir, si una herramienta informa de un elemento específico de seguridad, este dato será correcto al menos una vez; y 2) la tasa de falsos negativos es inferior al 100%, es decir, si tiene lugar un evento negativo relacionado con un elemento de seguridad específico, el servicio informará de dicho evento al menos una vez.

A.4 Requisitos de las capacidades en línea

A continuación se detallan los requisitos específicos de las capacidades en línea.

A.4.1 La capacidad en línea permitirá a un usuario encontrar elementos de seguridad conexos en su propio repositorio ("Búsqueda por CWE") mediante uno de los mecanismos siguientes: una función de búsqueda que localice identificadores CWE para elementos conexos, una correspondencia que vincule cada elemento con su identificador o identificadores CWE asociados, o cualquier otro mecanismo.

A.4.1.1 La capacidad en línea debería proporcionar una "plantilla" de la URL que permita a un programa informático construir fácilmente un enlace para acceder a la función de búsqueda, tal como se indica en el apartado A.4.1 anterior.

Ejemplos:

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

http://www.example.com/cwe/xxx.html

A.4.1.2 Si el sitio es de acceso público sin necesidad de registro, el programa CGI deberá aceptar el método "GET".

A.4.2 Para elaborar cualquier informe que identifique elementos de seguridad individuales, la capacidad en línea permitirá al usuario determinar los identificadores CWE asociados a dichos elementos ("Salida por CWE") mediante al menos uno de los siguientes mecanismos: permitir al usuario incluir identificadores CWE directamente en el informe, proporcionar al usuario una correspondencia entre los elementos de seguridad y los identificadores CWE, o utilizar cualquier otro mecanismo.

A.4.3 En la documentación pública de la capacidad se enumerarán explícitamente los identificadores CWE que el propietario considera cubiertos por el repositorio de la capacidad en línea ("cobertura declarada de compatibilidad CWE").

A.4.4 El sitio web público de la capacidad puede proporcionar la cobertura declarada de compatibilidad CWE en forma de uno o varios documentos XML de representación de declaración de cobertura (CCR) CWE.

A.4.5 Si la capacidad en línea no proporciona información detallada de los elementos de seguridad individuales, la capacidad en línea proporcionará una correspondencia que enlace cada elemento con su identificador o identificadores CWE asociados.

Anexo B

Requisitos de los medios

(Este anexo forma parte integrante de la presente Recomendación)

B.1 El medio de distribución utilizado por una capacidad compatible CWE utilizará uno de los formatos incluidos en el presente Anexo.

B.2 El formato de medios cumplirá sus requisitos específicos.

B.3 Documentos electrónicos (HTML, procesador de texto, PDF, texto ASCII, etc.)

B.3.1 El documento estará escrito en un formato comúnmente disponible que tenga lectores con funciones de tipo "encontrar" o "buscar" ("Búsqueda por CWE"), tales como texto ASCII, HTML o PDF.

B.3.2 Si el documento sólo proporciona nombres cortos o títulos para elementos individuales, enumerará los identificadores CWE relacionados con dichos elementos ("Salida por CWE").

B.3.3 El documento debería incluir una correspondencia entre los elementos y los identificadores CWE que enumere las páginas de cada elemento.

B.4 Interfaz gráfica de usuario (GUI)

A continuación se detallan los requisitos específicos de la interfaz gráfica de usuario.

B.4.1 La GUI proporcionará al usuario una función de búsqueda que le permita introducir el identificador CWE y recuperar los elementos conexos ("Búsqueda por CWE").

B.4.2 Si la GUI suministra información detallada sobre un elemento individual, enumerará los identificadores CWE que correspondan con dicho elemento ("Salida por CWE"). En caso contrario, la GUI proporcionará al usuario una correspondencia en un formato que cumpla el requisito de documento electrónico indicado en el apartado B.3.1.

B.4.3 La GUI debería permitir al usuario exportar o acceder a datos relacionados con la CWE en un formato alternativo que satisfaga el requisito de documentos electrónicos señalado en el apartado B.3.1.

Apéndice I

Lista de repositorios CWE para identificadores e información contextual conexa

(Este apéndice no forma parte integrante de la presente Recomendación)

MITRE Corporation	cwe.mitre.org/data

Apéndice II

Lista de autoridades de revisión

(Este apéndice no forma parte integrante de la presente Recomendación)

1. MITRE Corporation. Correo-e de contacto: cwe@mitre.org.

Bibliografia

[b-ITU-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2013