Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1526

(01/2014)

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

Intercambio de información de ciberseguridad – Intercambio de estados/vulnerabilidad

Lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema

Recomendación UIT-T X.1526

Unión Internacional de Telecomunicaciones

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/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1526

Lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema

Resumen

La Recomendación UIT-T X.1526 sobre el lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema (también conocido como lenguaje abierto de vulnerabilidades y evaluación, OVAL) incluye las tres fases principales del proceso de evaluación: representación de la información de configuración de los puntos extremos en cada prueba, análisis del punto extremo para la detección de los estados de máquina especificados (vulnerabilidad, configuración, parche, etc.) e información de los resultados de la evaluación. La finalidad de OVAL es proporcionar una norma comunitaria internacional sobre seguridad de la información para promover contenidos de seguridad abiertos y públicamente disponibles y normalizar la transferencia de esa información a través de toda la serie de instrumentos y servicios de seguridad. OVAL incluye un lenguaje utilizado para codificar los detalles del punto extremo, así como una compilación de repositorios de contenido a lo largo de toda la comunidad.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1526	2013-04-26	17	11.1002/1000/11752
2.0	ITU-T X.1526	2014-01-24	17	11.1002/1000/12039

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

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

Introducción

Esta Recomendación sobre el uso del lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema (también conocido como lenguaje abierto de vulnerabilidades y evaluación, OVAL) es una norma comunitaria internacional sobre seguridad de la información para promover contenidos de seguridad abiertos y públicamente disponibles, así como para normalizar la transferencia de dicha información a través de cualquier herramienta y servicio de seguridad. OVAL incluye un lenguaje para codificar el detalle de los puntos extremos y un conjunto de repositorios de contenidos diversos mantenidos por la comunidad. El lenguaje normaliza los tres principales pasos del proceso de evaluación: representación de la información de configuración de los puntos extremos en prueba, análisis del punto extremo para la detección de los estados de máquina especificados (vulnerabilidad, configuración, parche, etc.) e información de los resultados de la evaluación. Los repositorios son conjuntos de contenidos abiertos y públicamente disponibles que utilizan dicho lenguaje.

La comunidad OVAL ha desarrollado tres esquemas escritos en lenguaje de etiquetado extensible (*extensible markup language*, XML) para servir como marco y vocabulario del Lenguaje OVAL. Estos esquemas se corresponden con los tres pasos del proceso de evaluación: un esquema OVAL de Características del sistema para representar la información del punto extremo, un esquema OVAL de Definición para expresar un estado de máquina específico y un esquema OVAL de Resultados para informar acerca de los resultados de una evaluación.

Los contenidos escritos en Lenguaje OVAL están ubicados en uno de los numerosos repositorios que se encuentran dentro de la comunidad, uno de los cuales se conoce como Repositorio OVAL y es el principal lugar donde la Comunidad OVAL se reúne para debatir, analizar, almacenar y divulgar las definiciones OVAL. Cada definición del Repositorio OVAL determina si el punto extremo tiene o no una vulnerabilidad de software, un problema de configuración, programa o parche.

La comunidad de seguridad de la información contribuye al desarrollo de OVAL participando en la creación del Lenguaje OVAL sobre el Foro de Preparadores OVAL (OVAL *Developers Forum*) y escribiendo definiciones para el Repositorio OVAL por conducto del Foro de la Comunidad. La Junta de OVAL, integrada por representantes de una amplia gama de sectores de la industria, círculos académicos y organizaciones gubernamentales de todo el mundo, supervisa y aprueba el Lenguaje OVAL y controla la inclusión de definiciones en el sitio web de OVAL. De ese modo, OVAL es un reflejo de las opiniones y la competencia combinada de la mayor muestra posible de profesionales de la seguridad y la administración de sistemas procedentes de todo el mundo. La Recomendación UIT-T X.1526 ha sido elaborada teniendo en cuenta la importancia de mantener en la medida de lo posible la compatibilidad técnica entre la Recomendación UIT-T X.1526 y [b-MITRE Adoption].

Recomendación UIT-T X.1526

Lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema

1 Alcance

Esta Recomendación proporciona un medio estructurado para el intercambio mundial de contenidos de seguridad públicamente disponibles, así como para normalizar la transferencia de dicha información a través de cualquier herramienta y servicio de seguridad. El lenguaje para la definición abierta de vulnerabilidades y la evaluación del estado del sistema (también conocido como lenguaje abierto de vulnerabilidades y evaluación, OVAL) incluye un lenguaje para codificar el detalle de los puntos extremos y un conjunto de repositorios de contenidos diversos mantenidos por la comunidad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[ISO/IEC 19757-3] ISO/IEC 19757-3:2006, *Information technology – Document Schema Definition Language (DSDL) – Part 3: Rule-based validation – Schematron*.

3 Definiciones

3.1 Términos definidos en otros documentos

Esta Recomendación utiliza los siguientes términos definidos en otros documentos:

3.1.1 autoridad de revisión [b-UIT-T X.1520]: Cualquier entidad que realice una revisión.

NOTA – Actualmente MITRE es la única autoridad de revisión.

3.1.2 usuario [b-UIT-T X.1520]: Consumidor o potencial consumidor de la capacidad.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 instrumento de autoría (*authoring tool*): Producto que ayuda a crear nuevos ficheros OVAL (incluidos productos que consolidan las definiciones OVAL existentes en un solo fichero).

3.2.2 método de evaluación (*assessment method*): Método específico que un producto o servicio utiliza para evaluar una Definición de lenguaje abierto de vulnerabilidades y evaluación (OVAL). OVAL puede evaluarse mediante:

1) búsqueda en una base de datos de la configuración vigente de un punto extremo,
2) evaluación del estado por un sensor del anfitrión, o
3) evaluación del estado por un sensor distante.

3.2.3 capacidad (*capability*): Herramienta, base de datos, sitio web, recomendación o servicio de seguridad que proporciona una función de identificación de vulnerabilidad o exposición de seguridad.

3.2.4 prueba de corrección (*correctness testing*): Proceso encaminado a determinar si un producto, servicio o repositorio ha adoptado o no correctamente el lenguaje abierto de vulnerabilidades y evaluación (OVAL).

3.2.5 evaluador de definición (*definition evaluator*): Producto que utiliza una Definición de lenguaje abierto de vulnerabilidades y evaluación (OVAL) para orientar la evaluación y produce en consecuencia Resultados OVAL (completos).

3.2.6 repositorio de definición (*definition repository*): Repositorio de Definiciones de lenguaje abierto de vulnerabilidades y evaluación (OVAL) puesto a disponibilidad de la comunidad (gratuitamente o previo pago).

3.2.7 punto extremo (*endpoint*) (basado en la definición contemplada en [b-IETF RFC 5209]): todo dispositivo informático que puede conectarse a una red, como un ordenador, un servidor, un dispositivo de red, un dispositivo móvil, etc. Estos dispositivos suelen estar asociados a una dirección de capa de enlace concreta antes de sumarse a la red y, posiblemente también a una dirección IP una vez en la red.

3.2.8 propietario (*owner*) (basado en la definición contemplada en [b-UIT-T X.1520]): Propietario o quien mantiene la capacidad (según definición de la presente Recomendación).

3.2.9 producto (*product*): Aplicación, dispositivo o base de datos de seguridad que tiene una o más capacidades.

3.2.10 repositorio (*repository*) (basado en la definición contemplada en [b-UIT-T X.1520]): Conjunto implícito o explícito de elementos de seguridad que soporta una capacidad (según definición de la presente Recomendación), por ejemplo, una base de datos de vulnerabilidades, un fichero de recomendaciones, un conjunto de firmas en un sistema de detección de intrusiones (IDS, *intrusion detection system*) o un sitio web.

3.2.11 consumidor de resultados (*results consumer*): Producto que acepta los resultados de lenguaje abierto de vulnerabilidades y evaluación (OVAL) como insumo y muestra esos resultados al usuario o bien los utiliza para realizar alguna actividad (por ejemplo, reparación, gestión de la información de seguridad (SIM), etc.).

3.2.12 productor de características del sistema (*system characteristics producer*): Producto que genera un documento válido sobre características del sistema de lenguaje abierto de vulnerabilidades y evaluación (OVAL) sobre la base de los detalles de un sistema.

3.2.13 resultados de la prueba (*test results*): Datos que representan el resultado de las pruebas de corrección.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

CCE Enumeración de configuración común (*common configuration enumeration*)

CPE Enumeración de plataforma común (*common platform enumeration*)

CVE Vulnerabilidades y exposiciones comunes (*common vulnerabilities and exposures*)

ID Identificador (*identifier*)

SDI Sistema de detección de intrusión (*intrusión detection system*)

OVAL Lenguaje abierto de vulnerabilidades y evaluación (*open vulnerability and assessment language*)

SIM Gestión de la seguridad de la información (*security information management*)

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

5 Convenios

En esta Recomendación los términos "requerido", "debe", "no debe", "debería", "no debería", "recomendado", "puede" y "facultativo" se emplean conforme a la guía de estilo del UIT-T.

6 Requisitos de alto nivel

En los siguientes párrafos se definen los conceptos, funciones y responsabilidades en relación con las cinco capacidades diferentes, cada una de las cuales apunta a una utilización diferente del Lenguaje OVAL, que comprende la utilización adecuada de dicho lenguaje. Estas capacidades permiten a los miembros de la comunidad OVAL comprender fácilmente cómo utiliza un producto dado el Lenguaje OVAL y cómo éste podría ajustarse a sus necesidades.

Los siguientes requisitos se aplican a todas las capacidades que soportan OVAL, independientemente de la capacidad que prevean implementar. Si el producto, servicio o repositorio cumple con todos los requisitos aplicables, el propietario de la capacidad recibirá reconocimiento oficial de adopción correcta de OVAL.

Requisitos previos

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

6.2 El propietario de la capacidad acordará observar todos los requisitos de adopción de OVAL obligatorios, entre los cuales figuran los requisitos obligatorios para la capacidad específica.

6.3 El propietario de la capacidad le proporcionará a la autoridad de revisión los datos de un punto de contacto técnico calificado para responder preguntas sobre cualquier funcionalidad del producto, servicio o repositorio relacionada con OVAL, y coordinará la preparación del producto, servicio o repositorio para la prueba de corrección.

6.4 El propietario de la capacidad rellenará el formulario "Cuestionario sobre la adopción de OVAL" y se lo transmitirá a la autoridad de revisión. Este formulario se enviará una vez realizado satisfactoriamente el proceso de declaración. Para mayor información al respecto, tenga a bien dirigirse a la sección "Cómo declarar su producto, servicio o repositorio en calidad de adoptador de OVAL" en http://oval.mitre.org/adoption/requirements.html.

6.5 El propietario de la capacidad proporcionará a la autoridad de revisión libre acceso a los elementos necesarios para efectuar la prueba de corrección, con inclusión de los resultados de las pruebas y/o el repositorio, con miras a determinar el cumplimiento con todos los requisitos conexos.

6.6 El propietario de la capacidad colaborará con la autoridad de revisión con el fin de que el producto, servicio o repositorio esté disponible para la prueba de corrección.

6.7 Como parte de la recepción del reconocimiento oficial de la adopción correcta de OVAL, el propietario de la capacidad convendrá en respaldar a la autoridad de revisión en la realización de las actividades de prueba, e intercambiará los tipos de ficheros adecuados con otras organizaciones intentando demostrar la corrección de su producto, servicio o repositorio. Esto se realizará bajo la gestión de la autoridad de revisión y los esfuerzos de todos los involucrados se mantendrán a un nivel razonable.

6.8 El producto proporcionará valor o información adicional más allá de los proporcionados en el propio OVAL. Por consiguiente, para el reconocimiento oficial de la adopción correcta de OVAL no bastará con transmitir o proporcionar referencias a una sola fuente de Definiciones OVAL que hayan sido creadas por otros.

6.9 El producto, servicio o repositorio estará disponible para el público o un conjunto de consumidores.

6.10 El producto, servicio o repositorio indicará claramente el o los esquemas y versiones con los cuales es compatible.

Varios

6.11 Si la capacidad no satisface todos los requisitos aplicables indicados (cláusulas 6.1 a 6.10), el propietario de la capacidad no anunciará que es un adoptador de OVAL.

7 Corrección

La adopción de OVAL facilita la compatibilidad únicamente si la capacidad utiliza OVAL correctamente. Por lo tanto, las capacidades del adoptador de OVAL deben satisfacer los requisitos mínimos de corrección que se indican a continuación.

7.1 El propietario de la capacidad debe disponer de un medio para hacer que el usuario presente los errores de corrección encontrados en el uso de OVAL y en cualquier contenido OVAL producido por el producto, servicio o repositorio.

7.2 El propietario de la capacidad debe haber establecido un plan para corregir cualquier error de corrección que se le comunique.

7.3 El propietario de la capacidad debe corregir dentro de un período de tiempo razonable cualquier error de corrección que se le comunique.

8 Documentación

La documentación que se proporciona con un producto, servicio o repositorio de un adoptador de OVAL debe cumplir los siguientes requisitos.

8.1 El producto contendrá en su documentación una breve descripción de OVAL y de la adopción de OVAL, que puede estar basada en extractos literales de documentos del sitio web de OVAL.

8.2 El producto debe indicar claramente en su documentación cualesquiera pruebas individuales o esquemas de componentes que no soporte. Por ejemplo, si un producto, servicio o repositorio solicita que se le reconozca oficialmente haber adoptado correctamente OVAL como Evaluador de Definición y no soporta una prueba de características comerciales específicas del producto, entonces en la documentación de dicho producto, servicio o repositorio se debe declarar su incompatibilidad.

8.3 El producto o servicio indicará claramente en su documentación cuál(es) de los tres métodos de evaluación OVAL utiliza.

8.4 El producto, servicio o repositorio debe indicar claramente en su documentación el procedimiento que debe aplicar el usuario para presentar los errores de corrección encontrados en un contenido OVAL elaborado por el producto.

8.5 Si la documentación incluida con el producto, servicio o repositorio incluye un índice, éste debe contener referencias a documentación relacionada con OVAL bajo el término "OVAL".

9 Validez

Los adoptadores de OVAL deben trabajar con documentos válidos. Esto ayuda a garantizar que la información se formatea correctamente y que la estructura del documento se ajusta al Lenguaje OVAL.

9.1 El producto, servicio o repositorio validará todo el contenido OVAL (tanto el producido como el consumido) utilizando la validación de W3C XML schema, tomando como base la versión del Lenguaje OVAL que debe cumplir.

9.2 El producto, servicio o repositorio comunicará al usuario cualesquiera errores de validación de W3C XML schema.

9.3 El producto, servicio o repositorio validará todo el contenido OVAL (tanto el producido como el consumido) utilizando la validación Schematron [ISO/IEC 19757-3], tomando como base la versión del Lenguaje OVAL que debe cumplir.

9.4 El producto, servicio o repositorio comunicará al usuario cualesquiera errores de validación Schematron.

10 Requisitos de la capacidad específica

Los siguientes requisitos están relacionados con las capacidades de adopción específicas y sólo se aplican a los productos, servicios o repositorios que están tratando de obtener el reconocimiento oficial de haber adoptado correctamente OVAL para esa capacidad específica.

Instrumento de autoría	Producto que ayuda a crear nuevos ficheros OVAL (incluidos productos que consolidan las Definiciones OVAL existentes en un solo fichero).
Evaluador de definición	Producto que utiliza una Definición de OVAL para orientar la evaluación y produce en consecuencia Resultados OVAL (completos) utilizando uno o más de los métodos de evaluación de OVAL.
Repositorio de definición	Repositorio de Definiciones OVAL puesto a disponibilidad de la comunidad (gratuitamente o previo pago)
Consumidor de resultados	Producto que acepta los Resultados OVAL como insumo y muestra esos resultados al usuario o bien los utiliza para realizar alguna actividad (por ejemplo, reparación, gestión de la información de seguridad (SIM))
Productor de características del sistema	Producto que genera un documento válido sobre características del sistema OVAL sobre la base de los detalles de un punto extremo utilizando uno o más de los métodos de evaluación de OVAL

Productor de características del sistema

Estos requisitos se aplican a todos los productos o servicios que tienen el propósito de generar información sobre un punto extremo específico en el formato esquema de características del sistema OVAL.

10.1 El producto o servicio utilizará un identificador (ID) de punto único (único por fichero) para cada punto de características específicas del sistema que compile.

10.2 El producto o servicio generará puntos de características de sistema que contienen los valores de configuración de sistema exactos compilados en el momento en que el producto o servicio se ejecuta en el punto extremo.

10.3 El producto o servicio que utiliza un documento de Definición OVAL para generar puntos de características del sistema incluirá una sección collected_objects con un objeto de características del sistema por cada objeto compilado en el documento de Definición OVAL de entrada.

Repositorio de definición

Estos requisitos se aplican a todos los repositorios que tienen el propósito de proporcionar una compilación de información en el formato esquema de definición OVAL.

10.4 Todas las definiciones, pruebas, objetos, estados y variables OVAL contendrán un ID único con respecto de todas las otras definiciones, pruebas, objetos, estados y variables OVAL de la comunidad.

10.5 Cada repositorio deberá utilizar su propia porción espacio de nombres (*namespace*) constante única del ID a través de todos los contenidos OVAL.

10.6 Cada una de las definiciones, pruebas, objetos, estados y variables OVAL mantendrá el mismo ID durante toda su existencia. Esto permite a los usuarios referenciar estos puntos sobre la base de un ID estable. No se debería volver a escribir un punto existente con otra finalidad, pues los usuarios pueden haber referenciado ese punto en su propio contenido.

10.7 Cada actualización o modificación de una definición, prueba, objeto, estado o variable OVAL en el repositorio dará lugar a un incremento de la versión del punto. Análogamente, también se incrementará la versión de cada punto que referencie al punto actualizado o modificado. No es necesario que esta cascada de actualizaciones de versiones y puntos de referencia vaya más allá de la referencia Definiciones OVAL, pues ésta última proporciona una unidad lógica.

10.8 Los metadatos de Definición OVAL estarán en consonancia con el contenido de Definición OVAL (por ejemplo, si en la pruebas se está examinando 'platform white', la familia afectada no debería ser 'platform A'). Por otro lado, los metadatos reflejarán todo el contenido de Definición OVAL, lo que significa que los metadatos pueden necesitar secciones para cada familia afectada cuando una Definición OVAL se aplica a más de una familia.

10.9 Un repositorio que contiene una Definición OVAL para cubrir una vulnerabilidad específica incluirá como referencia, siempre que esté disponible, un nombre vulnerabilidades y exposiciones comunes (CVE).

10.10 Un repositorio que contiene una Definición OVAL para comprobar un estado de configuración específico incluirá como referencia, siempre que esté disponible, un ID enumeración de configuración común (CCE).

10.11 Un repositorio que contiene una Definición OVAL para comprobar una plataforma específica incluirá como referencia, siempre que esté disponible, un nombre enumeración de plataforma común (CPE).

10.12 El propietario de la capacidad documentará el proceso a tenor del cual un usuario puede recuperar actualizaciones de contenido.

Instrumento de autoría

Estos requisitos se aplican a todos los productos o servicios que están diseñados para facilitar la creación o modificación de contenido OVAL.

10.13 El instrumento de autoría proporcionará una interfaz de búsqueda que le permitirá al usuario buscar Definiciones, Pruebas, Objetos, Estados y Variables OVAL por ID.

10.14 El instrumento de autoría debería alentar la reutilización de las definiciones, pruebas, objetos, estados y variables OVAL existentes.

10.15 El instrumento de autoría debería permitirle al usuario invocar la validación en un documento que esté escrito para el Lenguaje OVAL y comunicarle al usuario todos los errores W3C XML schema y Schematron.

10.16 El instrumento de autoría le permitirá al usuario importar y editar el contenido OVAL existente.

10.17 El instrumento de autoría le permitirá al usuario exportar el contenido, creado por el instrumento, como documentos en Lenguaje OVAL válidos.

10.18 El instrumento de autoría le informará al usuario acerca de contenidos duplicados.

10.19 El instrumento de autoría proporcionará valor y capacidad por encima y más allá de la capacidad de un editor XML.

Evaluador de definición

Estos requisitos se aplican a todos los productos o servicios que tienen el propósito de evaluar un punto extremo especificado utilizando como insumo la información proporcionada en el formato OVAL *Definition schema*. Una vez realizada la evaluación, los Resultados se deben poner a disposición en el formato OVAL *results schema*.

10.20 El usuario estará en condiciones de determinar qué Definiciones OVAL se están evaluando.

10.21 El usuario estará en condiciones de examinar los detalles de cada Definición OVAL que se evalúa. Este requisito asegura que las Definiciones OVAL estén abiertas para el usuario, permitiéndole así observar cómo se somete a prueba una cuestión específica.

10.22 Si el producto o servicio no consume Definiciones OVAL durante el tiempo de ejecución, el propietario de la capacidad documentará el proceso mediante el cual un usuario puede presentar Definiciones OVAL al propietario de la capacidad para su interpretación por el producto. Esto incluye una indicación de la rapidez con la cual las definiciones presentadas al propietario de la capacidad se ponen a disposición del producto.

10.23 El producto o servicio será capaz de interpretar toda la lógica dentro de cada Definición OVAL y las Pruebas OVAL subsiguientes, de conformidad con los operadores lógicos declarados.

10.24 El producto o servicio determinará el resultado de la evaluación del punto extremo elegido sobre la base de los detalles especificados en la Definición OVAL.

10.25 El usuario será capaz de determinar el resultado de todas las Definiciones OVAL utilizadas en la evaluación del punto extremo elegido como objetivo.

10.26 El producto o servicio generará resultados exactos, predecibles y repetibles al utilizar un conjunto específico de Definiciones OVAL e información sobre el estado del punto extremo.

10.27 Los resultados generados por el producto o servicio estarán disponibles en el formato completo OVAL Results. Esto permite a otros productos o servicios que deseen aprovechar la información sobre evaluación detallada obtener la información deseada. También pueden ponerse a disposición resultados incompletos, pero se requieren resultados completos.

10.28 Cuando una Definición OVAL ha sido evaluada más de una vez en un único punto extremo, cada una de ellas con diferentes valores para las variables, el fichero OVAL Results incluirá valores de instancia variable única para cada uno de los casos.

10.29 El producto o servicio utilizará el resultado "no evaluada" para las Definiciones OVAL que forman parte del fichero original Definición OVAL pero que no son objeto de informe. Esto satisface el requisito 10.25 para la Definición OVAL dada.

10.30 Todo uso o traducción de una Definición OVAL al lenguaje interno del producto o servicio reflejará la misma lógica que la Definición OVAL original.

Consumidor de resultados

Estos requisitos se aplican a todos los productos o servicios que tienen el propósito de consumir información en el formato OVAL *Results schema*.

10.31 Para cada punto extremo definido en el fichero OVAL Result que se consume, el usuario será capaz de determinar las Definiciones OVAL específicas que son objeto de informe.

10.32 El usuario será capaz de examinar los detalles del fichero OVAL Results que se consume. Esto puede ser tan sencillo como permitirle al usuario abrir el fichero XML. La finalidad de este requisito es asegurar que los Resultados OVAL que se utilizan están abiertos para el usuario, permitiéndole así examinar los datos que son objeto de informe.

10.33 Si el producto o servicio no consume ficheros OVAL Results durante el tiempo de ejecución, el propietario documentará el proceso mediante el cual un usuario puede presentar ficheros OVAL

Results al propietario de la capacidad para su interpretación por el producto o servicio. Esto incluye una indicación de la rapidez con la cual las definiciones presentadas al propietario de la capacidad se ponen a disposición del producto o servicio.

11 Requisitos de la autoridad de revisión

Los siguientes requisitos pertenecen a la adopción de OVAL que debe respetar la autoridad de revisión.

11.1 La autoridad de revisión identificará claramente la versión de la adopción, la versión del documento de requisitos, y la versión del Lenguaje OVAL que se utilizó para determinar la observancia oficial de los requisitos de adopción de OVAL para cada producto, servicio o repositorio.

11.2 La autoridad de revisión definirá y publicará muestras de materiales de prueba.

11.3 La autoridad de revisión publicará información sobre la manera de participar en las pruebas de corrección de modo que las organizaciones puedan prepararse con la mayor antelación posible.

11.4 La autoridad de revisión proporcionará un punto de contacto para las pruebas de corrección respecto de las capacidades que declaran soporte de OVAL y hayan rellenado el formulario con el cuestionario para la adopción de OVAL ("OVAL *Adoption Questionnaire Form*").

11.5 La autoridad de revisión puede volver a someter a prueba un producto, servicio o repositorio que haya sido reconocido oficialmente como adoptador OVAL, si lo estima conveniente.

11.6 La autoridad de revisión debe proporcionar una copia del formulario de declaración de la adopción de OVAL a pedido de cualquier propietario de la capacidad válido que desee iniciar el Proceso de Adopción de OVAL.

11.7 La autoridad de revisión debe proporcionar una copia del formulario con el cuestionario para la adopción de OVAL a pedido de cualquier propietario de la capacidad válido que haya presentado un formulario de declaración de la adopción de OVAL.

12 Revocación

Si la autoridad de revisión verifica que un producto, servicio o repositorio ha adoptado correctamente OVAL, pero posteriormente tiene evidencias de que ya no se están observando los requisitos, podrá revocar su aprobación y ya no se reconocerá oficialmente que ese producto, servicio o repositorio ha adoptado correctamente OVAL. A continuación figuran los requisitos que debe tener en cuenta la autoridad de revisión para revocar el reconocimiento.

12.1 La autoridad de revisión proporcionará al propietario de la capacidad un aviso de revocación al menos dos (2) meses antes de la fecha en que esté prevista la revocación.

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

12.3 Si la autoridad de revisión concluye que las actuaciones o demandas del propietario son deliberadamente equivocadas, puede obviar el periodo de aviso. La autoridad de revisión puede interpretar como desee la expresión "deliberadamente equivocadas".

12.4 Si la autoridad de revisión concluye que las actuaciones del propietario de la capacidad en relación con los requisitos de adopción son deliberadamente equivocadas, la revocación debería estar vigente al menos un año.

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

12.6 Si el propietario de la capacidad considera que se cumplen los requisitos, puede responder al aviso de revocación proporcionando detalles específicos que demuestren por qué el producto, servicio o repositorio cumple los requisitos que han sido cuestionados.

12.7 Si durante el periodo de aviso el propietario modifica el producto, servicio o repositorio para que cumpla los requisitos cuestionados, la autoridad de revisión debería finalizar la actuación de revocación de dicho producto, servicio o repositorio.

12.8 La autoridad de revisión pondrá en público conocimiento que el reconocimiento oficial de la adopción correcta de OVAL ha sido revocado en relación con el producto, servicio o repositorio.

12.9 La autoridad de revisión podrá hacer públicas las razones de la revocación.

Bibliografía

[b-UIT-T X.1520] Recomendación UIT-T X.1520 (2014), *Vulnerabilidades y exposiciones comunes*.

[b-IETF RFC 5209] IETF RFC 5209 (2008), *Network Endpoint Assessment (NEA): Overview and Requirements*.

[b-MITRE Adoption] MITRE Corporation, Requisitos y Recomendaciones para la adopción y el uso de OVAL, versión 1.1 (22 de agosto de 2013). <http://oval.mitre.org/adoption/Requirements_and_Recommendations_for_OVAL_Adoption_and_Use_v1.1.pdf>

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, 2014