Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1520

(01/2014)

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

Intercambio de información de ciberseguridad – Intercambio de estados/vulnerabilidad

---

Vulnerabilidades y exposiciones comunes

Recomendación UIT-T X.1520

UIT-T

ITU 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.1520

Vulnerabilidades y exposiciones comunes

Resumen

Esta Recomendación sobre vulnerabilidades y exposiciones comunes (CVE, *common vulnerabilities and exposures*) ofrece una forma estructurada de intercambio de información de seguridad sobre vulnerabilidades y exposiciones con el objetivo de proporcionar nombres comunes para problemas conocidos públicamente en el área del software comercial o de fuente abierta utilizado en redes de comunicaciones, dispositivos de usuarios finales o en otros tipos de tecnologías de la información y las comunicaciones (TIC) que ejecutan programas informáticos. El objetivo de esta Recomendación es facilitar el intercambio de datos entre capacidades destinadas a combatir vulnerabilidades (herramientas, repositorios y servicios) empleando las denominaciones comunes incluidas en la misma. Esta Recomendación permite conectar bases de datos de vulnerabilidades y otras capacidades y facilitar la comparación de herramientas y servicios de seguridad. Por tanto, la Recomendación no incluye información sobre riesgos, impactos, información de parches o información técnica detallada, y sólo contiene el número identificador normalizado con indicador de estado, una breve descripción y referencias a informes y recomendaciones sobre vulnerabilidades conexas. El repositorio de identificadores CVE está disponible en cve.mitre.org/cve/cve.html.

Esta Recomendación pretende ser completa y abarcar todas las vulnerabilidades y exposiciones públicamente conocidas. Si bien se ha concebido para que incluya información que tenga un cierto grado de madurez, el objetivo básico es la identificación de vulnerabilidades y exposiciones detectadas mediante herramientas de seguridad, así como cualquier nuevo problema que se haga público y abordar antiguos problemas de seguridad que deban ser revisados.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1520	2011-04-20	17	11.1002/1000/11061
2.0	ITU-T X.1520	2014-01-24	17	11.1002/1000/12040

* 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 vulnerabilidades y exposiciones comunes (CVE, *common vulnerabilities and exposures*) presenta una forma estructurada de intercambio de información de seguridad sobre vulnerabilidades y exposiciones con el objetivo de proporcionar nombres comunes para problemas conocidos públicamente. El objetivo de la misma es facilitar el intercambio de datos entre capacidades destinadas a combatir vulnerabilidades (herramientas, repositorios y servicios) empleando las denominaciones comunes incluidas en la misma. Esta Recomendación permite conectar bases de datos de vulnerabilidades y otras capacidades y facilitar la comparación de herramientas y servicios de seguridad. Por tanto, la Recomendación no incluye información sobre riesgos, impactos, información de parches o información técnica detallada y sólo contiene el número identificador normalizado con indicador de estado, una breve descripción y referencias a informes y recomendaciones sobre vulnerabilidades conexas. El repositorio de identificadores CVE está disponible en http://cve.mitre.org/cve/cve.html.

Esta Recomendación pretende ser completa e incluir todas las vulnerabilidades y exposiciones públicamente conocidas. Si bien se ha concebido para que incluya información con un cierto grado de madurez, el objetivo básico es la identificación de vulnerabilidades y exposiciones detectadas mediante herramientas de seguridad y cualquier nuevo problema que se haga público, así como abordar antiguos problemas de seguridad que deban ser revisados.

Esta Recomendación forma parte de un conjunto de Recomendaciones del UIT-T originalmente elaboradas por una comunidad amplia y global de usuarios y desarrolladores que ha elaborado y hecho evolucionar una especificación abierta que se pone a disposición del UIT-T para su adopción con el acuerdo de que cualquier cambio o actualización de la misma garantice una equivalencia y compatibilidad técnica completa y que en los debates sobre sus modificaciones y mejoras se apliquen los procedimientos de la comunidad de usuarios original e incluyan referencias explícitas a la versión que mantenga la comunidad de usuarios.

Recomendación UIT-T X.1520

Vulnerabilidades y exposiciones comunes

1 Alcance

Esta Recomendación sobre la utilización de vulnerabilidades y exposiciones comunes proporciona una forma estructurada de intercambio global de información públicamente conocida sobre vulnerabilidades y exposiciones maduras que son detectadas mediante herramientas de seguridad o que se hacen públicas. Frecuentemente se hace referencia a dicha "forma estructurada" como "compatibilidad CVE" y define el uso correcto de CVE. Una vulnerabilidad de la seguridad de la información es un error del software que puede ser directamente utilizado por un pirata informático para acceder a un sistema o una red. Una exposición de la seguridad de la información es un error del software que permite el acceso a la información o a capacidades que puedan ser utilizadas por un pirata informático como punto de entrada a un sistema o una red. La asignación de identificadores de vulnerabilidades y exposiciones comunes (CVE) no está dentro del alcance de esta Recomendación.

La Recomendación UIT-T X.1520 se ha desarrollado en colaboración con MITRE Corporation, teniendo presente la importancia de mantener, en la medida de lo posible, la compatibilidad técnica entre la Recomendación UIT-T X.1520 y el Documento "*Requirements and Recommendations for CVE Compatibility*", de 30 de junio de 2013, disponible en el siguiente enlace: https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

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

3.2.2 capacidad: herramienta, base de datos, sitio web, recomendación o servicio de seguridad que proporciona una función de identificación de vulnerabilidad o exposición de seguridad.

3.2.3 exposición: una exposición de la seguridad de la información es un error en el software que permite acceder a información o capacidades que pueden ser utilizadas por un pirata informático como puerta de entrada a un sistema o una red.

3.2.4 mapa/correspondencia: especificación de las relaciones entre elementos de seguridad de un repositorio y los nombres CVE relacionados con dichos elementos.

3.2.5 propietario: el custodio (persona física o empresa) que asume la responsabilidad para la capacidad.

3.2.6 repositorio: conjunto implícito o explícito de elementos de seguridad que soporta una capacidad, 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.

3.2.7 revisión: proceso para determinar si una capacidad es compatibles con la CVE.

3.2.8 autoridad de revisión: cualquier entidad que realice una revisión.

NOTA – Actualmente MITRE es la única autoridad de revisión.

3.2.9 fecha de revisión: fecha del contenido CVE utilizado para determinar la compatibilidad CVE de una capacidad.

3.2.10 muestra de revisión: conjunto de elementos de seguridad en el repositorio de capacidades que utiliza la autoridad de revisión para evaluar la exactitud.

3.2.11 método de muestreo: método mediante el que la autoridad de revisión identifica el conjunto de elementos de seguridad de la muestra de revisión.

3.2.12 tamaño de muestra: porcentaje y/o número de elementos de seguridad que debe examinar la autoridad de revisión.

3.2.13 elemento de seguridad: registro de base de datos, mensaje de correo electrónico, recomendación de seguridad, sonda de evaluación, firma, etc., relacionada con una vulnerabilidad o exposición específica.

3.2.14 tarea: una sonda, verificación, firma, etc. de una herramienta que realiza una acción que genera información de seguridad (es decir, el elemento de seguridad).

3.2.15 herramienta: programa informático o dispositivo que examina a un anfitrión o a una red y genera información relacionada con vulnerabilidades o exposiciones o que agrega dicho tipo de información, por ejemplo, un explorador de vulnerabilidades, un sistema de detección de intrusiones, gestión de riesgos, gestor de información de seguridad o herramienta o servicio de informe de conformidad.

3.2.16 usuario: un consumidor o potencial consumidor de la capacidad.

3.2.17 vulnerabilidad: Una debilidad en el software que podría ser utilizada para violar un sistema o la información que contiene (basado en [b-UIT-T X.1500]).

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

ASCII Codificación normalizada americana para el intercambio de información (*american standard code for information interchange*)

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

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

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

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

IDS Sistema de detección de intrusiones (*intrusion detection system*)

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

POC Punto de contacto (*point of contact*)

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

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

5 Convenios

El término CVE se utiliza como un nombre en esta Recomendación.

6 Requisitos de alto nivel

Los elementos siguientes definen los conceptos, papeles y responsabilidades relativos a la utilización adecuada de identificadores CVE para que distintas capacidades destinadas a combatir las vulnerabilidades (herramientas, repositorios y servicios) puedan compartir datos con el fin de permitir la utilización común de bases de datos de vulnerabilidades y otras capacidades y facilitar el uso compartido de herramientas y servicios de seguridad.

Prerrequisitos

6.1 El propietario será una entidad legalmente válida, es decir, una organización o un individuo concreto con un número de teléfono, dirección de correo electrónico y domicilio postal válidos.

6.2 La capacidad proporcionará valor o información adicional a la proporcionada en la CVE (es decir, nombre, descripción, referencias y datos asociados).

6.3 El propietario proporcionará a la autoridad de revisión un punto de contacto técnico cualificado para responder a cuestiones relacionadas con la correspondencia y cualquier funcionalidad de la capacidad relativa a CVE.

6.4 La capacidad estará disponible para el público o para un conjunto de consumidores en una versión productiva.

6.5 El propietario proporcionará a la autoridad de revisión un "Formulario de evaluación de los requisitos de compatibilidad CVE " completo.

6.6 Si una capacidad dispone de un repositorio, el propietario proporcionará a la autoridad de revisión acceso libre al mismo para que pueda determinar si el repositorio satisface todos los requisitos.

6.7 Si una capacidad dispone de un repositorio, el propietario permitirá a la autoridad de revisión utilizar el repositorio para identificar vulnerabilidades que deban añadirse a las CVE.

6.8 El propietario se comprometerá a cumplir todos los requisitos de compatibilidad obligatorios de las CVE, incluyendo los requisitos obligatorios para el tipo concreto de capacidad.

Funcionalidad

6.9 La capacidad permitirá a los usuarios localizar los elementos de seguridad utilizando los nombres CVE ("búsqueda por CVE").

6.10 Cuando la capacidad presente elementos de seguridad al usuario, permitirá que éste obtenga los nombres CVE asociados ("salida de CVE").

6.11 Si una capacidad dispone de un repositorio, la correspondencia de la capacidad vinculará con precisión elementos de seguridad con los nombres CVE adecuados ("precisión del mapeo").

6.12 La documentación de la capacidad describirá adecuadamente la CVE, la compatibilidad de la CVE y cómo se utiliza en la capacidad la funcionalidad relacionada con la CVE ("documentación CVE").

6.13 La capacidad informará de su fecha de actualización con respecto a CVE ("fecha de uso").

6.14 La capacidad cumplirá cualquier requisito adicional para el tipo específico de capacidad, tal como se especifica en el Anexo A.

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

6.16 No se requiere que la capacidad haga lo siguiente:

- utilizar las mismas descripciones o referencias que la CVE;
- incluir cada nombre CVE en su repositorio.

Aspectos misceláneos

6.17 Si la capacidad no satisface todos los requisitos anteriores (del 6.1 al 6.16), el propietario no la anunciará como compatible con CVE.

7 Exactitud

La compatibilidad con CVE sólo permite el intercambio de datos si la correspondencia de la capacidad es exacta. Por tanto, las capacidades compatibles con CVE deben satisfacer requisitos mínimos de exactitud.

7.1 Si una capacidad dispone de un repositorio, éste tendrá un nivel de exactitud del 90% o superior.

7.2 Durante el periodo de revisión, el propietario corregirá cualquier error de correspondencia que detecte la autoridad de revisión.

7.3 Después del periodo de revisión, el propietario debería corregir cualquier error de correspondencia identificado tras un tiempo razonable desde que informó del mismo, es decir, en las siguientes dos (2) versiones del repositorio o seis (6) meses para las herramientas y tres (3) meses para capacidades y servicios en línea.

7.4 Si una capacidad dispone de un repositorio, el propietario debería elaborar y firmar una declaración en la que, hasta donde alcance su conocimiento, se afirme que la correspondencia no tiene errores.

7.5 Si la capacidad está basada o utiliza otra capacidad compatible con CVE (la capacidad "fuente"), y el propietario es consciente de errores de correspondencia en la capacidad fuente, el Propietario informará de dichos errores al Propietario de la capacidad fuente.

7.6 La exactitud de la correspondencia de los ficheros de recomendaciones se verificará con todos los elementos de seguridad del repositorio del fichero después de, e incluyendo, la primera utilización en el archivo de un nombre CVE en un elemento de seguridad.

7.7 Una capacidad reflejará con exactitud la situación de los nombres desaconsejados de las CVE en un plazo de tres (3) meses para las capacidades y servicios en línea.

7.8 Una capacidad no producirá ID de CVE desaconsejadas cuando se especifiquen ID más apropiadas en la descripción de la ID CVE desaconsejada en el plazo de tres (3) meses después de haberse desaconsejado la ID CVE.

8 Documentación

La documentación que se proporciona con la capacidad debe cumplir los requisitos siguientes.

8.1 La documentación incluirá una breve descripción de la CVE y de la compatibilidad de la CVE, que puede estar basada en extractos literales de documentos del sitio web de la CVE.

8.2 La documentación describirá cómo puede encontrar el usuario elementos de seguridad individuales en el repositorio de la capacidad utilizando nombres CVE.

8.3 La documentación describirá cómo puede el usuario obtener nombres CVE de elementos individuales en el repositorio de la capacidad.

8.4 Si la documentación incluye un índice, éste debería incluir referencias a la documentación asociada a la CVE bajo el término "CVE."

9 Fecha de uso (de la CVE)

Los usuarios deben conocer el grado de "actualización" del repositorio de una capacidad en lo relativo a su correspondencia con CVE. El propietario de la capacidad ha de indicar la vigencia de la correspondencia proporcionando la fecha de la última actualización de la información de la CVE e indica a los usuarios qué parte del contenido de la CVE utilizan y de dónde se ha recopilado el contenido de la CVE.

9.1 Cada nueva versión de la capacidad identificará la fecha más reciente del contenido CVE utilizada para crear o actualizar la correspondencia mediante al menos uno de los mecanismos siguientes: cambio de registros de acceso, listas de nuevas características, ficheros de ayuda u otro mecanismo. La capacidad se "actualiza" con respecto a dicha fecha.

9.2 Cada nueva versión de la capacidad se actualizará en relación con una fecha de CVE declarada que no sea anterior en más de tres (3) meses a la disponibilidad de la capacidad para los usuarios. Si una capacidad no satisface este requisito se considera que está "desactualizada".

9.3 El propietario hará pública la frecuencia con que actualizará el repositorio de la capacidad para incluir nueva información de la CVE.

9.4 El propietario describirá los criterios y mecanismos para seleccionar la información CVE incluida en una capacidad.

9.5 El propietario informará la fuente de la que recopila nuevos contenidos CVE.

10 Distintos estilos de soporte de la denominación de la CVE

Una capacidad trabajará con nombres CVE con independencia del formato de la representación del nombre CVE en la capacidad, con independencia de que esté trabajando con la sintaxis del antiguo estilo CVE-ID de cuatro dígitos o la sintaxis de longitud variable (cuatro dígitos o más) (utilizada después de la modificación de la sintaxis CVE-ID en vigor después del 30 de diciembre de 2013).

10.1 Si un usuario realiza una búsqueda utilizando YYYY-NNNN, YYYY-NNNNN, YYYY-NNNNNN u otra ID válida con un mayor número de dígitos, la capacidad devolverá los elementos de seguridad que se correspondan respectivamente con CVE-YYYY-NNNN, CVE-YYYY-NNNNN, CVE-YYYY-NNNNNN u otra ID válida con un mayor número de dígitos en su repositorio, con independencia de que el nombre CVE incluya en su nombre CVE o CAN.

10.2 Si la capacidad contiene un nombre CVE del tipo CVE-YYYY-NNNN, pero el usuario hace la búsqueda utilizando el formato antiguo del nombre CVE, es decir, CAN-YYYY-NNNN (utilizado antes de la modificación del esquema de nombres CVE del 19 de octubre de 2005), la capacidad debería devolver CVE-YYYY-NNNN.

11 Revocación de la compatibilidad CVE

11.1 Si una autoridad de revisión ha verificado que una capacidad es compatible con CVE, pero ulteriormente tiene evidencias de que no se cumplen los 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 frase "deliberadamente equivocadas" como considere oportuno.

11.3 Salvo que lo recomienden dos miembros de la Comisión Editorial de la CVE que no tengan conflictos de intereses, la autoridad de revisión no debería considerar la revocación de la compatibilidad CVE para una capacidad determinada en más de una ocasión cada seis (6) meses.

Aviso y evaluación

11.4 La autoridad de revisión proporcionará al propietario de la capacidad y al punto técnico de contacto una aviso de revocación al menos dos (2) meses antes de la fecha en que esté prevista la revocación.

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 porqué la capacidad cumple los requisitos que han sido cuestionados.

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

Revocación

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

11.8 La autoridad de revisión hará pública la revocación de compatibilidad CVE para dicha capacidad.

11.9 Si la autoridad de revisión concluye que las actuaciones del propietario en relación con los requisitos de compatibilidad de la CVE son deliberadamente equivocados, la revocación debería estar vigente al menos un año.

11.10 La autoridad de revisión podrá hacer públicas las razones de una revocación.

11.11 Si se revoca la aprobación, el propietario no podrá solicitar una nueva revisión durante el periodo de revocación.

12 Autoridad de revisión

En cualquier revisión que realice la autoridad de revisión:

12.1 La autoridad de revisión analizará la compatibilidad CVE para una fecha específica del contenido CVE, es decir, la fecha de revisión.

12.2 La autoridad de revisión identificará claramente la fecha de revisión utilizada para establecer la compatibilidad de la capacidad.

12.3 La autoridad de revisión identificará claramente la versión del documento de requisitos de compatibilidad de la CVE utilizado para establecer la compatibilidad de la capacidad.

12.4 La autoridad de revisión definirá y hará público un tamaño de muestra.

12.4.1 La autoridad de revisión debería utilizar un tamaño de muestra de 50 elementos más el 5% del repositorio de la capacidad, hasta una muestra de 400 elementos como máximo.

12.4.2 La autoridad de revisión puede analizar cada elemento de entrada del repositorio de la capacidad.

12.5 La autoridad de revisión hará público el método de muestreo.

12.6 La autoridad de revisión podrá utilizar una muestra de revisión no seleccionada al azar.

12.7 La autoridad de revisión utilizará el mismo método de muestreo y tamaño de muestra en todas las evaluaciones de capacidad que realice en un periodo de tiempo determinado.

Anexo A

Requisitos específicos de los tipos de capacidades

(Este anexo forma parte integral de la presente Recomendación.)

Dado que existe una amplia variedad de capacidades que utilizan la CVE, algunos tipos de capacidades pueden tener características singulares que precisen una atención especial en relación con la compatibilidad CVE.

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

A.1.1 Si la capacidad es un sistema de exploración para la evaluación de vulnerabilidades, un sistema de detección de intrusiones (IDS) o un producto que integre los resultados de uno o más sistemas de exploración e IDS, debe satisfacer 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 gestionado de detección y respuesta a intrusiones, o un servicio de exploración a distancia), debe satisfacer 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 de vulnerabilidades o de firmas en línea, un fichero en web o un sitio para mantenimiento/parches, debe satisfacer los requisitos de las capacidades en línea, es decir, de A.4.1 a A.4.3.

A.1.4 Si la capacidad es una herramienta de agregación tal como un gestor de información de seguridad, una herramienta de información de conformidad o un servicio que suministre dichas agregaciones de información de tipos de vulnerabilidades, debe satisfacer los requisitos de las capacidades de agregación, es decir, de A.5.1 a A.5.6.

Requisitos de las herramientas

A.2.1 La herramienta permitirá al usuario utilizar los nombres CVE para localizar tareas asociadas en dicha herramienta ("búsqueda por CVE") proporcionando al menos uno de los mecanismos siguientes: función "buscar" o "encontrar", correspondencia entre dichos nombres de tareas de herramientas y nombres CVE, u otro mecanismo.

A.2.2 Para cualquier informe que identifique elementos de seguridad individuales, la herramienta permitirá al usuario determinar los nombres CVE asociados a dichos elementos ("salida por CVE") mediante al menos uno de los mecanismos siguientes: inclusión de nombres CVE directamente en el informe, correspondencia entre dichos nombres de tareas de herramientas y nombres CVE u otro mecanismo.

A.2.3 Cualquier informe o correspondencia que sea necesaria satisfará los requisitos de medios especificados en el Anexo B.

A.2.4 La herramienta, o el propietario, deberían proporcionar al usuario una lista con todos los nombres CVE asociados con las tareas de la herramienta.

A.2.5 La herramienta debería permitir al usuario seleccionar un conjunto de tareas proporcionando un fichero que contenga una lista de nombres CVE.

A.2.6 La interfaz de la herramienta debería permitir al usuario visualizar, seleccionar y descartar un conjunto de tareas utilizando nombres CVE individuales.

A.2.7 Si la herramienta no tiene una tarea que esté asociada con un nombre CVE tal como haya especificado el usuario en los requisitos de herramienta A.2.5 o A.2.6, la herramienta debería notificar al usuario que no puede realizar la tarea asociada.

A.2.8 El propietario garantizará que: 1) la tasa de falsos positivos es inferior al 100%, es decir, si la herramienta informa de un elemento de seguridad específico, éste será correcto al menos una vez; y 2) la tasa de falsos negativos es inferior al 100%, es decir, si ocurre un evento relacionado con un elemento de seguridad específico, al menos una vez la herramienta informará de dicho evento.

Requisitos de los servicios de seguridad

Los servicios de seguridad pueden utilizar en su actividad herramientas compatibles con CVE, pero no pueden ofrecer a sus clientes acceso directo a dichas herramientas. Por tanto, puede resultar difícil a los clientes identificar y comparar las capacidades de distintos servicios. Los Requisitos de los servicios de seguridad abordan esta potencial limitación.

A.3.1 El servicio de seguridad deberá poder utilizar nombres CVE para indicar al usuario qué elementos de seguridad ha probado o detectado el servicio ("búsqueda por CVE") mediante uno o más de los mecanismos siguientes: proporcionar al usuario una lista de nombres CVE que identifiquen los elementos probados o detectados por el servicio, proporcionar al usuario una correspondencia entre los elementos del servicio y los nombres CVE, responder a una lista de nombres CVE facilitada por un usuario con la identificación de qué nombres han sido probados o detectados por el servicio, o utilizar cualquier otro mecanismo.

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

A.3.3 Cualquier informe o correspondencia necesaria proporcionada por el servicio cumplirá los requisitos de medios especificados en el Anexo B.

A.3.4 Si el servicio proporciona al usuario acceso directo a un producto que identifique elementos de seguridad, el producto debería ser compatible con CVE.

A.3.5 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, éste será correcto al menos una vez; y 2) la tasa de falsos negativos es inferior al 100%, es decir, si tiene lugar un evento que esté relacionado con un elemento de seguridad específico, el servicio informará de dicho evento al menos una vez.

Requisitos de las capacidades en línea

A.4.1 Una capacidad en línea permitirá a un usuario encontrar elementos de seguridad conexos en el repositorio de la capacidad en línea ("búsqueda por CVE ") mediante uno de los mecanismos siguientes: una función de búsqueda que devuelva nombres CVE para elementos conexos, una correspondencia que vincule cada elemento con su nombre o nombres CVE asociados, o cualquier otro mecanismo.

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

Ejemplos:
```
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNN
http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY NNNNNN
http://www.example.com/cve/CVE-YYYY-NNNN.html
```

A.4.1.2 Si la plantilla de la URL es para un programa CGI, el programa debería aceptar el método HTTP "GET".

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

A.4.3 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 nombre o nombres CVE asociados.

Requisitos de las capacidades de agregación

A.5.1 La capacidad de agregación permitirá al usuario utilizar nombres CVE para localizar elementos asociados en dicha capacidad ("búsqueda por CVE ") mediante al menos uno de los mecanismos siguientes: una función "encontrar" o "buscar", una correspondencia entre dichos nombres de capacidad y los nombres CVE, u otro mecanismo con la aprobación de la Autoridad de revisión.

A.5.2 Para cualquier informe que identifique elementos de seguridad individuales, la capacidad de agregación permitirá al usuario determinar los nombres CVE asociados a dichos elementos ("salida por CVE") mediante al menos uno de los mecanismos siguientes: incluir nombres CVE directamente en el informe, proporcionar una correspondencia entre los nombres de la capacidad y nombres CVE, o utilizar cualquier otro mecanismo.

A.5.3 Cualquiera de los informes o correspondencias requeridas cumplirán los requisitos de medios especificados en el Anexo B.

A.5.4 La herramienta o el propietario, deberían proporcionar al usuario una lista de todos los nombres CVE asociados a las tareas de la herramienta.

A.5.5 La herramienta debería permitir al usuario seleccionar un conjunto de tareas mediante un fichero que contenga una lista de nombres CVE.

A.5.6 La interfaz de la herramienta debería permitir al usuario visualizar, seleccionar y descartar un conjunto de tareas utilizando nombres CVE individuales.

Anexo B

Requisitos de los medios

(Este anexo forma parte integral de la presente Recomendación.)

B.1 El medio de distribución utilizado por una capacidad compatible con CVE utilizará uno de los formatos de medios incluidos en este anexo.

B.2 El formato de medios cumplirá los requisitos específicos de dicho formato.

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 CVE"), tales como texto ASCII, HTML o PDF.

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

B.3.3 El documento debería incluir una correspondencia entre elementos y nombres CVE, que enumere las páginas de cada elemento.

Interfaz gráfica de usuario (GUI)

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

B.4.2 Si la GUI enumera la información detallada de un elemento individual, enumerará el nombre o nombres CVE que se correspondan con dicho elemento ("salida por CVE"). En cualquier otro caso, la GUI proporcionará al usuario una correspondencia en un formato que cumpla el requisito de documentos electrónicos señalado en B.3.1.

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

Anexo C

Requisitos de los medios

(Este anexo forma parte integral de la presente Recomendación.)

El actual esquema XML de CVE está disponible en: http://cve.mitre.org/schema/cve/cve_1.0.xsd y se replica a continuación.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns="http://cve.mitre.org/cve/downloads/1.0"
    targetNamespace="http://cve.mitre.org/cve/downloads/1.0"
    elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <!--  ********************************************************************** -->
  <!--  Changelog: 1.0 - Initial version -->
  <!--  ********************************************************************** -->
  <xsd:annotation>
    <xsd:documentation xml:lang="en">
      Simple schema that defines the format of the CVE List provided by MITRE
    </xsd:documentation>
  </xsd:annotation>

  <!--  ********************************************************************** -->
  <!--  Start Item Element Definition -->
  <!--  ********************************************************************** -->
  <xsd:element name="cve">
    <xsd:annotation>
      <xsd:documentation xml:lang="en">
        cve is the top level element of the CVE List provided by MITRE.
        It represents holds all CVE Items.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="item" type="ItemType" minOccurs="1" maxOccurs="unbounded"/>
      </xsd:sequence>
      <xsd:attribute name="schemaVersion" type="xsd:token" use="optional"/>
    </xsd:complexType>
  </xsd:element>

  <!--  ********************************************************************** -->
  <!--  Simple Types -->
  <!--  ********************************************************************** -->
  <!-- CUSTOM TYPE DEFINITIONS-->
  <xsd:simpleType name="typeEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="CAN"/>
      <xsd:enumeration value="CVE"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="statusEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Entry"/>
      <xsd:enumeration value="Candidate"/>
    </xsd:restriction>
  </xsd:simpleType>

  <!-- need to verify enumeration -->
  <xsd:simpleType name="simplePhaseEnumType">
    <xsd:restriction base="xsd:token">
      <xsd:enumeration value="Proposed"/>
      <xsd:enumeration value="Interim"/>
      <xsd:enumeration value="Modified"/>
      <xsd:enumeration value="Assigned"/>
    </xsd:restriction>
  </xsd:simpleType>
```

```
<!--  ********************************************************************** -->
<!--  Complex Types -->
<!--  ********************************************************************** -->
<xsd:complexType name="ItemType">
  <xsd:sequence>
    <xsd:element name="status" type="statusEnumType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="phase" type="specificPhaseType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="desc" type="xsd:string" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="refs" type="refsType" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="votes" type="votesType" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="comments" type="commentsType" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <!--Need to Verify Enumeration-->
  <xsd:attribute name="type" type="typeEnumType" use="required"/>
  <xsd:attribute name="name" type="xsd:token" use="required"/>
  <xsd:attribute name="seq" type="xsd:token" use="required"/>
</xsd:complexType>

<xsd:complexType name="commentsType">
  <xsd:sequence>
    <xsd:element name="comment" minOccurs="0" maxOccurs="unbounded">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="voter" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="votesType">
  <xsd:sequence>
    <xsd:element name="accept" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="modify" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="noop" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="recast" minOccurs="0" maxOccurs="1">
      <xsd:complexType>
        <xsd:simpleContent>
          <xsd:extension base="xsd:string">
            <xsd:attribute name="count" type="xsd:token" use="required"/>
          </xsd:extension>
        </xsd:simpleContent>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="reject" minOccurs="0" maxOccurs="1">
```

```
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="reviewing" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="revote" minOccurs="0" maxOccurs="1">
        <xsd:complexType>
          <xsd:simpleContent>
            <xsd:extension base="xsd:string">
              <xsd:attribute name="count" type="xsd:token" use="required"/>
            </xsd:extension>
          </xsd:simpleContent>
        </xsd:complexType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="specificPhaseType">
    <xsd:simpleContent>
      <xsd:extension base="simplePhaseEnumType">
        <xsd:attribute name="date" type="xsd:token" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="refsType">
    <xsd:annotation>
      <xsd:documentation>holds all hyperlink elements</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="ref" type="refType" minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="refType">
    <xsd:annotation>
      <xsd:documentation>Holds individual hyperlink element</xsd:documentation>
    </xsd:annotation>
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="source" type="xsd:token" use="required"/>
        <xsd:attribute name="url" type="xsd:anyURI" use="optional"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
</xsd:schema>
```

Bibliografía

[b-UIT-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, 2014