Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1526

(01/2014)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange concernant les vulnérabilités/les états

Langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système

Recommandation UIT-T X.1526

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	**X.1520–X.1539**
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1526

Langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système

Résumé

La Recommandation UIT-T X.1526 sur le langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système (également appelé langage ouvert d'évaluation de la vulnérabilité (OVAL, *open vulnerability and assessment language*)) englobe les trois principales étapes du processus d'évaluation: la représentation des informations de configuration des points d'extrémité à tester; l'analyse du point d'extrémité en vue de détecter un état précis de la machine (en ce qui concerne la vulnérabilité, la configuration, un correctif, etc.); et le compte-rendu des résultats de cette évaluation. OVAL a pour objet de fournir une norme communautaire internationale en matière de sécurité de l'information, qui vise à promouvoir des contenus ouverts et publiquement accessibles sur la sécurité et à normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité. Par OVAL, on entend le langage employé pour coder des informations précises sur les points d'extrémité, mais aussi un ensemble de divers répertoires de contenus, tenus dans l'ensemble de la communauté.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
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

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

La Recommandation UIT-T X.1526, qui décrit l'utilisation du langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système (également appelé langage ouvert d'évaluation de la vulnérabilité (OVAL, *open vulnerability and assessment language*)), est une norme communautaire internationale en matière de sécurité de l'information, qui vise à promouvoir des contenus ouverts et publiquement accessibles sur la sécurité et à normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité. Par OVAL, on entend le langage employé pour coder des informations précises sur les points d'extrémité, mais aussi un ensemble de divers répertoires de contenus, tenus dans l'ensemble de la communauté. Le langage permet de normaliser les trois principales étapes du processus d'évaluation: la représentation des informations de configuration des points d'extrémité à tester; l'analyse du point d'extrémité en vue de détecter un état précis de la machine (en ce qui concerne la vulnérabilité, la configuration, un correctif, etc.); et le compte-rendu des résultats de cette évaluation. Les répertoires sont des recueils de contenus accessibles au public et ouverts, qui utilisent le langage.

La communauté OVAL a mis au point trois schémas employant le langage de balisage extensible (XML, *extensible markup language*), destinés à être le cadre et le vocabulaire du langage OVAL. Ces schémas correspondent aux trois étapes du processus d'évaluation: un schéma pour les caractéristiques du système OVAL, permettant de représenter des informations sur les points d'extrémité, un schéma pour les définitions OVAL, permettant de décrire l'état précis de la machine et un schéma pour les résultats OVAL, permettant de rendre compte des résultats de l'évaluation.

Les contenus en langage OVAL sont placés dans l'un des nombreux répertoires de la communauté. Un tel répertoire est nommé répertoire OVAL. Il est le lieu central où se rencontre la communauté OVAL pour discuter, analyser, archiver et diffuser des définitions OVAL. Chaque définition dans le répertoire OVAL permet de déterminer si une vulnérabilité de logiciel, un problème de configuration, un programme ou un correctif spécifique est présent dans un point d'extrémité.

La communauté chargée de la sécurité de l'information contribue à la mise en place d'OVAL en participant à l'élaboration du langage OVAL sur le forum des développeurs OVAL et en formulant des définitions pour le répertoire OVAL, par l'entremise du forum de la communauté OVAL. Un comité OVAL, composé de représentants d'un large éventail d'entreprises, d'établissements universitaires et d'organisations gouvernementales du monde entier, supervise et approuve OVAL et surveille l'affichage des définitions hébergées sur le site web OVAL. Par conséquent, OVAL reflète les idées mais aussi l'expérience du plus large ensemble possible de professionnels dans le domaine de la sécurité et de l'administration des systèmes dans le monde entier. La Recommandation UIT-T X.1526 a été élaborée sans perdre de vue qu'il était important de maintenir, dans la mesure du possible, la compatibilité sur le plan technique avec [b-MITRE Adoption].

Recommandation UIT-T X.1526

Langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système

1 Domaine d'application

La présente Recommandation sur le langage pour la définition ouverte des vulnérabilités et pour l'évaluation de l'état d'un système (également appelé langage ouvert d'évaluation de la vulnérabilité (OVAL, *open vulnerability and assessment language*)) a pour objet de fournir un moyen structuré permettant d'échanger à l'échelle mondiale des contenus publiquement accessibles sur la sécurité et de normaliser le transfert de ces informations à l'ensemble des outils et des services de sécurité. Par OVAL, on entend le langage employé pour coder des informations précises sur les points d'extrémité, mais aussi un ensemble de divers répertoires de contenus, tenus dans l'ensemble de la communauté.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[ISO/CEI 19757-3] ISO/CEI 19757-3:2006, *Technologies de l'information – Langages de définition de schéma de documents (DSDL) – Partie 3: Validation de règles orientées – Schematron*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 autorité d'examen [b-UIT-T X.1520]: toute entité qui procède à un examen.

NOTE – MITRE est la seule autorité d'examen à ce jour.

3.1.2 utilisateur [b-UIT-T X.1520]: consommateur ou consommateur potentiel de la capacité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 outil de création: produit qui contribue au processus de création de nouveaux fichiers en langage ouvert d'évaluation de la vulnérabilité (OVAL) (notamment les produits qui regroupent les définitions OVAL existantes en un fichier unique).

3.2.2 méthode d'évaluation: méthode particulière qu'un produit ou un service utilise pour évaluer une définition en langage ouvert d'évaluation de la vulnérabilité (OVAL). OVAL prend en charge l'évaluation de la manière suivante:

1) interrogation d'une base de données des paramètres de configuration existants d'un point d'extrémité;
2) évaluation de l'état par un capteur situé sur le serveur; ou

3) évaluation de l'état par un capteur à balayage existant.

3.2.3 capacité: fonction(s) spécifique(s) d'un produit, d'un service ou d'un répertoire.

3.2.4 vérification d'adoption correcte: processus permettant de déterminer si un produit, un service ou un répertoire adopte correctement le langage ouvert d'évaluation de la vulnérabilité (OVAL).

3.2.5 évaluateur de définition: produit qui emploie une définition en langage ouvert d'évaluation de la vulnérabilité (OVAL) pour guider l'évaluation et qui fournit des résultats OVAL (résultats complets).

3.2.6 répertoire de définitions: répertoire de définitions en langage ouvert d'évaluation de la vulnérabilité (OVAL), rendu accessible à la communauté (gratuitement ou moyennant paiement).

3.2.7 point d'extrémité (d'après la définition donnée dans [b-IETF RFC 5209]): dispositif informatique quelconque pouvant être connecté à un réseau, par exemple système informatique, serveur, appareil de réseau, dispositif mobile, etc. "Ces dispositifs sont en règle générale associés à une adresse de couche de liaison donnée avant d'intégrer le réseau et, éventuellement, à une adresse IP une fois situés sur le réseau."

3.2.8 propriétaire: (sur la base de la définition donnée dans [b-UIT-T X.1520]): gardien (personne réelle ou entreprise) en charge de la capacité (telle que définie dans la présente Recommandation).

3.2.9 produit: application de sécurité, appareil ou base de données de sécurité qui présente une ou plusieurs capacités.

3.2.10 répertoire (sur la base de la définition donnée dans [b-UIT-T X.1520]): recueil implicite ou explicite d'éléments de sécurité, qui vient à l'appui d'une capacité (telle que définie dans la présente Recommandation), par exemple une base de données de vulnérabilités, une archive de conseils, l'ensemble des signatures d'un système de détection des intrusions (IDS, *intrusion detection system*) ou un site web.

3.2.11 consommateur de résultats: produit qui accepte les résultats en langage ouvert d'évaluation de la vulnérabilité (OVAL) en entrée et montre ces résultats à l'utilisateur ou les emploie pour exécuter une action (p.ex. correction, gestion des informations de sécurité (SIM, *security information management*)).

3.2.12 producteur de caractéristiques du système: produit qui génère un document valable en langage ouvert d'évaluation de la vulnérabilité (OVAL) sur les caractéristiques d'un système, sur la base d'informations précises concernant le système.

3.2.13 résultats de test: données obtenues lors de la vérification d'adoption correcte.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

CCE liste des configurations courantes (*common configuration enumeration*)

CPE liste des plates-formes courantes (*common platform enumeration*)

CVE vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)

ID identificateur (*identifier*)

IDS système de détection des intrusions (*intrusion detection system*)

OVAL langage ouvert d'évaluation de la vulnérabilité (*open vulnerability and assessment language*)

SIM gestion des informations de sécurité (*security information management*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Les mots clés "requis", "doit", "ne doit pas", "devrait", "ne devrait pas", "recommandé", "peut" et "facultatif" utilisés dans la présente Recommandation sont interprétés conformément au guide des auteurs de l'UIT-T.

6 Exigences de haut niveau

Les points suivants définissent les concepts, les rôles et les responsabilités, associés aux cinq différentes capacités, chacune ciblant un usage différent du langage OVAL, et un usage approprié s'entend. Ces capacités permettent aux membres de la communauté OVAL de comprendre facilement comment un produit donné emploie le langage OVAL et comment il pourrait répondre à leurs besoins.

Les exigences suivantes s'appliquent à toutes les capacités qui prennent en charge OVAL, quelle que soit la capacité qu'il est prévu d'implémenter. Si le produit, le service ou le répertoire satisfait à toutes les exigences applicables, le propriétaire de la capacité recevra une attestation de reconnaissance officielle de l'adoption correcte d'OVAL.

Conditions préalables

6.1 Le propriétaire de la capacité doit être une entité juridique valable, c'est-à-dire un organisme ou une personne particulière, possédant un numéro de téléphone, une adresse électronique et une adresse postale valables.

6.2 Le propriétaire de la capacité doit accepter de se soumettre à toutes les exigences obligatoires relatives à l'adoption d'OVAL, notamment celles qui concernent la capacité en question.

6.3 Le propriétaire de la capacité doit communiquer à l'autorité d'examen un point de contact technique qui est qualifié pour répondre aux questions concernant une quelconque fonctionnalité OVAL du produit, du service ou du répertoire, et pour coordonner la préparation du produit, du service ou du répertoire en vue de la vérification d'adoption correcte.

6.4 Le propriétaire de la capacité doit faire parvenir à l'autorité d'examen un "Questionnaire relatif à l'adoption d'OVAL" dûment rempli. Ce formulaire doit être envoyé dès que la procédure de déclaration aura été achevée. Pour de plus amples informations, veuillez-vous reporter à la section intitulée "How to Declare Your Product, Service, or Repository as an OVAL Adopter" (*Comment, en tant qu'adoptant, déclarer votre produit, service ou répertoire*) à l'adresse: http://oval.mitre.org/adoption/requirements.html.

6.5 Le propriétaire de la capacité doit faire en sorte que l'autorité d'examen ait un libre accès aux éléments nécessaires à la vérification d'adoption correcte, notamment les résultats des tests et/ou le répertoire, afin d'évaluer la conformité avec toutes les exigences associées.

6.6 Le propriétaire de la capacité doit collaborer avec l'autorité d'examen, dans le but de mettre le produit, le service ou le répertoire à disposition pour une vérification d'adoption correcte.

6.7 En vue de recevoir une attestation de la reconnaissance officielle de l'adoption correcte d'OVAL, le propriétaire de la capacité doit accepter d'apporter son appui à l'autorité d'examen lors du prolongement des activités de test, lorsque des types appropriés de fichiers seront échangés avec d'autres organismes afin d'essayer de prouver l'adoption correcte d'OVAL par leur produit, service ou répertoire. Ceci se fera sous la direction de l'autorité d'examen et n'exigera des participants que des efforts raisonnables.

6.8 Le produit doit fournir des valeurs ou des informations qui vont au-delà de celles qui sont fournies dans le cadre d'OVAL même. Donc, le transfert ou la fourniture d'une référence à une source unique de définitions OVAL qui ont été établies par quelqu'un d'autre n'est en lui-même pas considéré comme étant suffisant pour la reconnaissance officielle de l'adoption correcte d'OVAL.

6.9 Le produit, le service ou le répertoire doit être accessible au public ou à un ensemble de consommateurs.

6.10 Le produit, le service ou le répertoire doit clairement mentionner le ou les schémas et la version avec lesquels il est compatible.

Divers

6.11 Si la capacité ne satisfait pas à toutes les exigences applicables susmentionnées (§ 6.1 à 6.10), son propriétaire ne doit pas annoncer qu'il a adopté OVAL.

7 Adoption correcte

L'adoption d'OVAL ne facilite l'interopérabilité que si l'emploi d'OVAL par la capacité est correct. En conséquence, les capacités de l'adoptant d'OVAL doivent satisfaire aux exigences minimales décrites ci-après.

7.1 Le propriétaire de la capacité doit prévoir un moyen permettant à l'utilisateur de présenter les erreurs reflétant une adoption incorrecte qu'il a repérées dans l'utilisation d'OVAL et dans un quelconque contenu OVAL fourni par le produit, le service ou le répertoire.

7.2 Le propriétaire de la capacité doit prévoir un plan lui permettant de rectifier les erreurs reflétant une adoption incorrecte qui lui sont signalées.

7.3 Le propriétaire de la capacité doit rectifier les erreurs reflétant une adoption incorrecte qui lui sont signalées dans un délai raisonnable à compter du signalement initial de l'erreur.

8 Documentation

Les exigences suivantes s'appliquent à la documentation qui est fournie avec un produit, un service ou un répertoire de l'adoptant d'OVAL.

8.1 La documentation du produit doit comporter une description succincte d'OVAL et de l'adoption d'OVAL, qui peut contenir des parties reprises mot pour mot de documents placés sur le site web OVAL.

8.2 La documentation du produit doit clairement indiquer tout schéma de composante ou tout test individuel que le produit n'accepte pas. Par exemple, si un produit demande, en tant qu'évaluateur de définition, une reconnaissance officielle de l'adoption correcte d'OVAL et qu'il n'accepte pas un test de fonctionnalité de produit commercial spécifique, alors la documentation du produit, du service ou du répertoire doit mentionner cette incompatibilité.

8.3 La documentation du produit ou du service doit clairement indiquer quelle(s) méthode(s) d'évaluation, parmi les trois prises en charge par OVAL, le produit ou le service utilise.

8.4 La documentation du produit, du service ou du répertoire doit clairement indiquer la procédure qu'un utilisateur doit suivre pour présenter les erreurs reflétant une adoption incorrecte qu'il a repérées dans un quelconque contenu OVAL fourni par le produit.

8.5 Si la documentation accompagnant le produit, le service ou le répertoire comporte un index, celui-ci doit contenir des références, en regard de la rubrique "OVAL", à la documentation relative à OVAL.

9 Validité

Les adoptants d'OVAL sont tenus d'employer des documents valables. Cela contribue à ce que les informations soient correctement formatées et à ce que la structure du document suive le langage OVAL.

9.1 Le produit, le service ou le répertoire doit, au moyen de la validation selon le schéma XML du W3C, valider tout contenu OVAL (tant produit que consommé) en le comparant à la version du langage OVAL à laquelle il est déclaré être conforme.

9.2 Le produit, le service ou le répertoire doit signaler à l'utilisateur toute erreur de validation dans le cadre du schéma XML du W3C.

9.3 Le produit, le service ou le répertoire doit, au moyen de la validation Schematron [ISO/CEI 19757-3], valider tout contenu OVAL (tant produit que consommé) en le comparant à la version du langage OVAL à laquelle il est déclaré être conforme.

9.4 Le produit, le service ou le répertoire doit signaler à l'utilisateur toute erreur de validation dans le cadre du Schematron.

10 Exigences concernant des capacités spécifiques

Les exigences suivantes se rapportent à des capacités spécifiques liées à l'adoption d'OVAL et ne s'appliquent qu'aux produits, aux services et aux répertoires qui cherchent à obtenir la reconnaissance officielle de leur adoption correcte d'OVAL pour cette capacité spécifique.

Outil de création	Produit qui contribue au processus de création de nouveaux fichiers OVAL (notamment les produits qui regroupent les définitions OVAL existantes en un fichier unique).
Evaluateur de définition	Produit qui emploie une définition OVAL pour guider l'évaluation et qui fournit des résultats OVAL (résultats complets), en utilisant une ou plusieurs des méthodes d'évaluation prises en charge par OVAL.
Répertoire de définitions	Répertoire de définitions OVAL, rendu accessible à la communauté (gratuitement ou moyennant paiement).
Consommateur de résultats	Produit qui accepte les résultats OVAL en entrée et montre ces résultats à l'utilisateur ou les emploie pour exécuter une action (p.ex. correction, gestion des informations de sécurité (SIM, *security information management*)).
Producteur de caractéristiques du système	Produit qui génère un document OVAL valable sur les caractéristiques d'un système, sur la base d'informations précises concernant un point d'extrémité, en utilisant une ou plusieurs des méthodes d'évaluation prises en charge par OVAL.

Producteur de caractéristiques du système

Ces exigences s'appliquent à tous les produits ou services qui envisagent de générer des informations sur un point d'extrémité spécifique au format du schéma pour les caractéristiques du système OVAL.

10.1 Le produit ou le service doit employer un identificateur (ID) unique (par fichier) pour chacun des éléments de la caractéristique du système qu'il recueille.

10.2 Le produit ou le service doit générer des éléments de la caractéristique du système qui contiennent les valeurs exactes de la configuration du système, recueillies au moment où le produit ou le service est fourni au point d'extrémité.

10.3 Le produit ou le service qui emploie un document de définition OVAL pour générer des éléments de caractéristique doit inclure une section collected_objects avec l'objet de la caractéristique du système pour chaque objet recueilli dans le document de définition OVAL d'entrée.

Répertoire de définitions

Ces exigences s'appliquent à tous les répertoires qui envisagent de fournir un ensemble d'informations au format du schéma pour les définitions OVAL.

10.4 L'ensemble des définitions, des tests, des objets, des états ou des variables OVAL doit contenir un identificateur unique dans l'ensemble des définitions, tests, objets, états et variables de la communauté OVAL.

10.5 Chacun des répertoires doit employer sa partie constante et unique d'espace de nom de l'identificateur dans l'ensemble des contenus OVAL.

10.6 Chacun des définitions, des tests, des objets, des états ou des variables OVAL conserve le même identificateur tout au long de son existence. Cela permet aux utilisateurs de faire référence à ces éléments en se fondant sur un identificateur stable. Un élément existant ne devrait pas être réinscrit à d'autres fins puisque les utilisateurs peuvent y faire référence dans leur propre contenu.

10.7 Chacune des mises à jour ou modifications dans le répertoire des définitions, des tests, des objets, des états ou des variables OVAL doit conduire à l'incrémentation de la version de l'élément. De même, la version de tout élément qui fait référence à l'élément mis à jour ou modifié fera l'objet d'une incrémentation. Cette répercussion des mises à jour des versions sur les éléments s'y référant ne doit pas s'étendre au-delà de la référence aux définitions OVAL puisque les définitions OVAL fournissent une unité logique.

10.8 Les métadonnées sur les définitions OVAL doivent correspondre aux contenus des définitions OVAL (par exemple, la famille affectée ne devrait pas être la "plate-forme A" si les tests examinent la "plate-forme blanche"). En outre, les métadonnées doivent correspondre à tous les contenus des définitions OVAL, et doivent en conséquence peut-être inclure des sections pour chaque famille affectée lorsque la définition OVAL s'applique à plus d'une famille.

10.9 Un répertoire qui contient une définition OVAL dans le but de décrire une vulnérabilité spécifique doit inclure, s'il est disponible, un nom de vulnérabilités et d'expositions courantes (CVE, *common vulnerabilities and exposures*) en tant que référence.

10.10 Un répertoire qui contient une définition OVAL dans le but de vérifier si l'état est un état de configuration spécifique doit inclure, s'il est disponible, un identificateur de liste de configurations courantes (CCE, *common configuration enumeration*) en tant que référence.

10.11 Un répertoire qui contient une définition OVAL dans le but de vérifier si une plate-forme est une plate-forme spécifique doit inclure, s'il est disponible, un nom de liste de plateformes courantes (CPE, *common platform enumeration*) en tant que référence.

10.12 Le propriétaire de la capacité doit décrire la procédure au moyen de laquelle un utilisateur peut récupérer des mises à jour de contenus.

Outil de création

Ces exigences s'appliquent à tous les produits ou services qui sont conçus pour faciliter la création ou la modification de contenus OVAL.

10.13 Un outil de création doit fournir une interface de recherche permettant à l'utilisateur de rechercher des définitions, des tests, des objets, des états ou des variables OVAL au moyen de leur identificateur.

10.14 Un outil de création devrait encourager à la réutilisation des définitions, des tests, des objets, des états ou des variables OVAL existants.

10.15 Un outil de création devrait permettre à l'utilisateur d'invoquer la validation d'un document qui est écrit pour le langage OVAL et signaler à l'utilisateur toutes les erreurs dans le schéma XML de W3C et le Schematron.

10.16 Un outil de création doit permettre à l'utilisateur d'importer et d'éditer des contenus OVAL existants.

10.17 Un outil de création doit permettre à l'utilisateur d'exporter les contenus créés au moyen de l'outil, en tant que documents valables en langage OVAL.

10.18 Un outil de création devrait signaler les contenus en double à l'utilisateur.

10.19 Un outil de création doit fournir la valeur et la capacité au-dessus et au-delà de la capacité d'un éditeur XML.

Evaluateur de définition

Ces exigences s'appliquent à tous les produits ou services qui envisagent d'évaluer un point d'extrémité spécifié au moyen, en entrée, d'informations fournies dans le format de schéma pour les définitions OVAL. Une fois l'évaluation faite, les résultats doivent être mis à la disposition au format du schéma pour les résultats OVAL.

10.20 L'utilisateur doit être en mesure de déterminer les définitions OVAL qui sont évaluées.

10.21 L'utilisateur doit être en mesure d'examiner les détails de chacune des définitions OVAL qui sont évaluées. Cette exigence garantit que les définitions OVAL sont ouvertes à l'utilisateur, lui permettant de voir comment un problème spécifique est éprouvé.

10.22 Si le produit ou le service ne consomme pas de définitions OVAL pendant l'exécution, le propriétaire de la capacité doit décrire la procédure au moyen de laquelle un utilisateur peut lui soumettre des définitions OVAL pour interprétation par le produit. Il convient de mentionner avec quelle rapidité les définitions présentées au propriétaire de la capacité seront à la disposition du produit.

10.23 Le produit ou le service doit être en mesure d'interpréter toute la logique dans chaque définition OVAL et les tests subséquents, à l'aide des opérateurs logiques déclarés.

10.24 Le produit ou le service doit déterminer le résultat de l'évaluation du point d'extrémité cible sur la base des détails spécifié dans la définition OVAL.

10.25 L'utilisateur doit être en mesure de déterminer le résultat de toutes les définitions OVAL lors de l'évaluation du point d'extrémité cible.

10.26 Le produit ou le service doit produire des résultats précis, prévisibles et reproductibles lorsqu'il emploie un ensemble spécifique de définitions OVAL et des informations sur l'état du point d'extrémité.

10.27 Les résultats générés par le produit ou le service doivent être mis à la disposition au format pour les résultats OVAL complets. Cela permet à d'autres produits ou services qui veulent exploiter des informations détaillées sur l'évaluation, d'obtenir les informations souhaitées. Des résultats partiels peuvent être disponibles aussi, mais les résultats complets sont exigés.

10.28 Lorsqu'une définition OVAL a été évaluée plus d'une fois pour un seul point d'extrémité, chaque fois avec des valeurs différentes pour les variables, le fichier des résultats OVAL doit contenir, pour chaque cas, les valeurs uniques d'instance de la variable.

10.29 Un produit ou service doit employer un résultat de "non évalué" pour toutes les définitions OVAL qui sont contenues dans le fichier original des définitions OVAL mais ne font pas l'objet d'un compte-rendu. Cela satisfait à l'exigence du § 10.25 pour la définition OVAL donnée.

10.30 Toute utilisation ou traduction d'une définition OVAL en un langage interne du produit ou du service doit faire apparaître la même logique que la définition OVAL initiale.

Consommateur de résultats

Ces exigences s'appliquent à tous les produits ou services qui envisagent de consommer des informations au format du schéma pour les résultats OVAL.

10.31 Pour chaque point d'extrémité défini dans le fichier des résultats OVAL consommé, l'utilisateur doit être en mesure de déterminer les définitions OVAL spécifiques qui font l'objet d'un compte rendu.

10.32 L'utilisateur doit être en mesure d'examiner les détails du fichier des résultats OVAL consommé. Cela peut se borner à autoriser l'utilisateur à ouvrir le fichier XML. Le but de cette exigence est de s'assurer que les résultats OVAL utilisés sont ouverts à l'utilisateur et lui permettent d'examiner les données dont il est rendu compte.

10.33 Si le produit ou le service ne consomme pas de fichiers de résultats OVAL pendant l'exécution, le propriétaire doit décrire la procédure au moyen de laquelle un utilisateur peut lui soumettre des fichiers de résultats OVAL pour interprétation par le produit ou le service. Il convient de mentionner avec quelle rapidité les fichiers présentés au propriétaire de la capacité seront à la disposition du produit ou du service.

11 Exigences concernant l'autorité d'examen

Ci-après sont données les exigences relatives à l'adoption OVAL auxquelles l'autorité d'examen doit satisfaire.

11.1 L'autorité d'examen doit clairement identifier la version de l'adoption, la version du document contenant les exigences et la version du langage OVAL qui a été employé pour déterminer s'il a été satisfait officiellement aux exigences concernant l'adoption OVAL pour chaque produit, chaque service ou chaque répertoire.

11.2 L'autorité d'examen doit définir et publier des exemples de matériels de test.

11.3 L'autorité d'examen doit diffuser des informations sur la manière de participer à la vérification d'adoption correcte, de manière que les organisations puissent se préparer autant que possible d'avance.

11.4 L'autorité d'examen doit fournir un point de contact en vue d'organiser la vérification d'adoption correcte pour les capacités déclarant prendre en charge OVAL pour lesquelles le questionnaire relatif à l'adoption d'OVAL ("OVAL Adoption Questionnaire Form") a été rempli.

11.5 L'autorité d'examen peut, à sa discrétion, resoumettre à un test un produit, un service ou un répertoire qui a été officiellement reconnu comme ayant adopté OVAL.

11.6 L'autorité d'examen doit fournir une copie de la déclaration d'adoption d'OVAL à tout propriétaire de capacité valable souhaitant débuter le processus d'adoption d'OVAL qui en aura fait la demande.

11.7 L'autorité d'examen doit fournir une copie du questionnaire relatif à l'adoption d'OVAL à tout propriétaire de capacité ayant soumis une déclaration d'adoption d'OVAL remplie qui en aura fait la demande.

12 Révocation

Si l'autorité d'examen a vérifié qu'un produit, un service ou un répertoire a correctement adopté OVAL, mais que plus tard elle a la preuve que les exigences ne sont plus respectées, elle peut révoquer son approbation et le produit, le service ou le répertoire ne sera plus officiellement reconnu comme ayant correctement adopté OVAL. Ci-après sont données les exigences auxquelles l'autorité d'examen doit satisfaire en vue de révoquer la reconnaissance.

12.1 L'autorité d'examen doit adresser au propriétaire de la capacité un avertissement de révocation au moins deux (2) mois avant la date prévue pour la révocation.

12.2 L'autorité d'examen peut reporter la date de révocation.

12.3 Si l'autorité d'examen constate que les actions ou les déclarations du propriétaire de la capacité sont intentionnellement de nature à induire en erreur, elle peut ne pas tenir compte de la période de préavis. L'autorité d'examen peut interpréter l'expression "intentionnellement de nature à induire en erreur" comme elle l'entend.

12.4 Si l'autorité d'examen estime que les actions du propriétaire de la capacité, en ce qui concerne les exigences relatives à l'adoption, sont intentionnellement de nature à induire en erreur, la révocation doit s'étendre sur une année au moins.

12.5 L'autorité d'examen doit identifier les exigences spécifiques qui ne sont pas respectées.

12.6 Si le propriétaire de la capacité estime qu'il est satisfait aux exigences, il doit répondre à l'avertissement de révocation en fournissant des détails précis indiquant pourquoi le produit, le service ou le répertoire satisfait auxdites exigences.

12.7 Si le propriétaire modifie le produit, le service ou le répertoire au cours de la période de préavis de manière qu'il satisfasse auxdites exigences, l'autorité d'examen devrait mettre un terme au processus de révocation pour le produit, le service ou le répertoire.

12.8 L'autorité d'examen doit rendre public le fait que la reconnaissance officielle de l'adoption correcte d'OVAL a été révoquée pour le produit, le service ou le répertoire.

12.9 L'autorité d'examen peut rendre publics les motifs de révocation.

Bibliographie

[b-UIT-T X.1520] Recommandation UIT-T X.1520 (2014), *Vulnérabilités et expositions courantes*.

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

[b-MITRE Adoption] MITRE Corporation, Requirements and Recommendation for OVAL Adoption and Use, Ver. 1.1 (22 août 2013).
<http://oval.mitre.org/adoption/Requirements_and_Recommendations_for_OVAL_Adoption_and_Use_v1.1.pdf>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2014