Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1524

(03/2012)

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

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

Liste des failles courantes

Recommandation UIT-T X.1524

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

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

Recommandation UIT-T X.1524

Liste des failles courantes

Résumé

La Recommandation UIT-T X.1524 sur l'emploi de la liste des failles courantes (CWE, *common weakness enumeration*) contient une méthode structurée, permettant de s'échanger les failles en matière de sécurité dans les informations, qui fournit les noms courants des problèmes connus du public, présents dans les logiciels commerciaux ou libres, utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final ou dans tout autre équipement employant la technologie de l'information et de la communication (TIC), qui assure l'exploitation d'un logiciel. La liste CWE a pour objet de rendre possible une discussion, une description, un choix et un emploi plus efficaces d'outils et de services de sécurité logicielle, qui permettent de repérer les failles dans le code source et dans les systèmes opérationnels, ainsi qu'une compréhension et une gestion meilleures des failles logicielles liées à l'architecture et à la conception. La présente Recommandation indique comment employer la liste CWE pour mettre au point un système permettant d'employer simultanément les outils et les services de sécurité logicielle, les connaissances de base en la matière et d'autres capacités, et pour faciliter la comparaison desdits outils et services de sécurité. La liste CWE offre aussi des informations complémentaires sur les risques éventuels, les impacts, la résolution, et des informations techniques détaillées sur les conséquences possibles des failles logicielles pour un système logiciel.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1524	2012-03-02	17

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 concernant la liste des failles courantes (CWE, *common weakness enumeration*) décrit l'utilisation des listes des failles courantes et contient une méthode structurée, permettant de s'échanger des ensembles unifiés et mesurables de failles logicielles, qui a pour but de fournir les noms courants des problèmes connus du public. La liste CWE vise, d'une part, à rendre possible une discussion, une description, un choix et un emploi plus efficaces d'outils et de services de sécurité logicielle, qui permettent de repérer les failles dans le code source et dans les systèmes opérationnels et, d'autre part, à promouvoir une compréhension et une gestion meilleures des failles logicielles liées à l'architecture et à la conception.

L'objectif de la liste CWE est d'être exhaustif pour ce qui est des causes des vulnérabilités et des expositions connues du public, qu'il s'agisse de failles dans l'architecture, la conception, le code ou le déploiement du logiciel. Tandis que la liste CWE est conçue pour contenir des informations solides, elle a pour principal objet de recenser les failles qui peuvent engendrer des vulnérabilités et des expositions. L'autorité d'examen détermine la conformité de l'emploi des identificateurs CWE, tels que définis dans la présente Recommandation.

La liste CWE s'appuie sur des travaux existants menés au sein de la communauté de la cybersécurité, notamment le grand nombre de vulnérabilités diverses rencontrées dans la pratique, qui sont spécifiées dans la Recommandation UIT-T X.1520 – Vulnérabilités et expositions courantes (CVE, *common vulnerabilities and exposures*). Nombre de sources et d'exemples sont employés pour établir les définitions spécifiques et succinctes des éléments de la liste CWE et des structures arborescentes de classification. En outre, des mappages appropriés sont créés entre les éléments CWE et les identifiants CVE, de manière que chaque identificateur CWE corresponde à une liste d'identifiants CVE spécifiques appartenant à une catégorie CWE particulière de failles en matière de sécurité logicielle. En établissant la liste CWE et l'arborescence de classification, on cherche à couvrir au maximum les domaines théoriques, commerciaux et techniques appropriés.

La présente Recommandation est techniquement équivalente à la version 1.0 du document relatif aux prescriptions et recommandations concernant la compatibilité et l'efficacité CWE (*Requirements and Recommendations for CWE compatibility and effectiveness*), daté du 28 juillet 2011 https://cwe.mitre.org/compatible/requirements_v1.0.html.

Recommandation UIT-T X.1524

Liste des failles courantes

1 Domaine d'application

La présente Recommandation sur l'emploi de la liste des failles courantes (CWE, *common weakness enumeration*) contient une "méthode structurée", permettant de s'échanger à l'échelle mondiale des informations concernant les failles en matière de sécurité logicielle dans l'architecture, la conception, le code ou le déploiement, qui peuvent ôter aux systèmes logiciels leur sécurité, leur fiabilité et leur invulnérabilité face aux attaques. Des outils de sécurité, des services d'évaluation et certains types d'examen de sécurité peuvent repérer ces types de failles logicielles. Cette "méthode structurée", souvent nommée "compatibilité avec la liste CWE", définit l'utilisation correcte de la liste CWE. Une faille en matière de sécurité dans les informations est une erreur dans le logiciel qui peut conduire à une vulnérabilité susceptible d'être employée par un pirate pour accéder à un système ou à un réseau. L'attribution d'identificateurs CWE sort du cadre de la présente Recommandation. Une liste des répertoires d'identificateurs CWE et des informations corollaires associées figure dans l'Appendice I.

L'objectif de la liste CWE, dont l'emploi est décrit dans la présente Recommandation, est d'être exhaustive pour ce qui est de l'architecture logicielle, la conception, le codage et les erreurs de déploiement qui sont la cause profonde des vulnérabilités et des expositions. Tandis que la liste CWE est conçue pour contenir des informations solides, elle a pour principal objet de recenser, de faire connaître et de décrire cette cause profonde des vulnérabilités et des expositions, de manière que celles-ci puissent être évitées par les développeurs, éprouvées pour les équipes de développement et gérées par elles, et être systématiquement signalées par les outils et les services de sécurité.

La présente Recommandation est techniquement équivalente à la version 1.0 du document relatif aux prescriptions et recommandations concernant la compatibilité et l'efficacité CWE (*Requirements and Recommendations for CWE compatibility and effectiveness*), daté du 28 juillet 2011 https://cwe.mitre.org/compatible/requirements_v1.0.html.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 précision (en pourcent): pourcentage d'éléments de sécurité dans l'échantillon d'examen, qui renvoient aux identificateurs CWE corrects.

3.2.2 instrument: outil d'évaluation, environnement de développement intégré (IDE, *integrated development environment*), outil d'examen des codes, compilateur de vérification des codes, base de données, site web, conseil ou service fournissant des informations sur les failles au niveau de l'implémentation, la conception ou l'architecture, qui peuvent conduire à une vulnérabilité, exploitable en matière de sécurité, dans le logiciel.

3.2.3 formulaire d'évaluation des prescriptions en matière de compatibilité avec la liste CWE: formulaire d'évaluation qui contient une série de questions visant à ce que le propriétaire de l'instrument prouve, à l'aide de références à des textes, des images ou des sites web, que son instrument est conforme aux prescriptions en matière de compatibilité définies dans la présente Recommandation, ainsi que des instructions sur l'endroit où déposer le formulaire rempli ou pour demander à l'autorité d'examen des précisions sur la façon de remplir le formulaire d'évaluation.

3.2.4 formulaire d'évaluation des prescriptions en matière d'efficacité par rapport à la liste CWE: formulaire d'évaluation qui contient une série de questions visant à ce que le propriétaire de l'instrument prouve, à l'aide de références à des textes, des images ou des sites web, que son instrument est conforme aux prescriptions en matière d'efficacité définies dans la présente Recommandation, ainsi que des instructions sur l'endroit où déposer le formulaire rempli, la demande d'essai ou pour demander à l'autorité d'examen des précisions sur la façon de remplir le formulaire d'évaluation.

3.2.5 essai d'efficacité: processus permettant de déterminer si un instrument est efficace par rapport à la liste CWE.

3.2.6 mise en correspondance/mappage: spécification des relations entre les éléments faibles dans un répertoire et les identificateurs CWE qui sont liés à ces éléments.

3.2.7 propriétaire: gardien (personne réelle ou société) en charge de l'instrument.

3.2.8 répertoire: ensemble implicite ou explicite d'éléments logiciels faibles en matière de sécurité, qui vient à l'appui d'un instrument, par exemple une base de données des failles en matière de sécurité, l'ensemble des configurations dans un analyseur de codes ou un site web.

3.2.9 examen: processus permettant de déterminer si un instrument est compatible avec la liste CWE.

3.2.10 autorité d'examen: autorité qui procède à un examen ou à un essai d'efficacité et est autorisée à accorder le statut de compatibilité avec la liste CWE (compatibilité CWE) ou celui d'efficacité par rapport à la liste CWE (efficacité CWE).

A noter que l'Appendice II contient une liste des autorités d'examen.

3.2.11 version de l'examen: version datée de la liste CWE qui est employée pour déterminer la compatibilité avec ladite liste ou l'efficacité par rapport à elle d'un instrument.

3.2.12 élément de sécurité: enregistrement dans une base de données, sonde d'évaluation, signature, etc., qui est lié(e) à une faille particulière en matière de sécurité.

3.2.13 mission: sonde, vérification, signature, etc., par un outil, qui exécute une action produisant des informations sur la sécurité (par exemple un élément de sécurité).

3.2.14 résultats d'essai: données correspondant aux résultats des essais d'efficacité.

3.2.15 outil: application ou dispositif logiciel qui examine une portion logicielle, une portion binaire ou un autre phénomène parasite et produit des informations sur la sécurité, par exemple un analyseur de la sécurité du code source, un outil d'évaluation de la qualité du code, un compilateur de vérification du code ou un environnement de développement.

3.2.16 utilisateur: consommateur ou consommateur potentiel de l'instrument.

3.2.17 vulnérabilité: toute faille dans le logiciel qui peut être exploitée pour violer un système ou les informations qu'il contient (sur la base de la Recommandation UIT-T X.1500).

3.2.18 faille: lacune ou imperfection dans le code logiciel, la conception, l'architecture ou le déploiement, qui peut, à un moment donné, devenir une vulnérabilité ou peut contribuer à l'introduction d'autres vulnérabilités.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

ASCII american standard code for information interchange

CCR représentation de déclaration de couverture (*coverage claim representation*)

CGI interface de passerelle commune (*common gateway interface*)

CWE liste des failles courantes (*common weakness enumeration*)

GUI interface graphique utilisateur (*graphical user interface*)

HTML langage de balisage hypertexte (*hypertext markup language*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

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

POC point de contact (*point of contact*)

URL localisateur uniforme de ressource (*uniform resource locator*)

TIC technologies de l'information et de la communication

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

5 Conventions

Aucune.

6 Prescriptions de haut niveau

Les points suivants définissent les concepts, les rôles et les responsabilités liés à la bonne utilisation des identificateurs CWE lors du partage des données entre les instruments différents de détection des failles en matière de sécurité (outils, répertoires et services) pour permettre auxdits instruments d'être employés ensemble et pour faciliter la comparaison des outils et des services de détection des failles en matière de sécurité.

6.1 Le propriétaire de l'instrument 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 L'instrument doit fournir des valeurs ou des informations supplémentaires qui vont au-delà de ce qui est fourni dans la liste CWE elle-même (à savoir, le nom, la description, les risques, les références et les informations associées sur les failles).

6.3 Le propriétaire de l'instrument doit communiquer à l'autorité d'examen un point de contact technique qui est qualifié pour répondre aux questions liées à la précision du mappage, à toute fonctionnalité liée à la liste CWE de l'instrument, et pour coordonner l'essai de l'instrument venant à l'appui de l'évaluation de son efficacité à identifier les éléments CWE.

6.4 L'instrument doit être mis à la disposition du public ou d'un ensemble de consommateurs, dans une version prototype ou une version publique, en étant par exemple disponible sur un site web public, pour une utilisation libre, à la vente ou en tant que service fourni dans le cadre d'un contrat.

6.5 Pour être compatible avec la liste CWE, le propriétaire de l'instrument doit faire parvenir à l'autorité d'examen un "formulaire d'évaluation des prescriptions en matière de compatibilité avec la liste CWE" dûment rempli.

6.6 Le propriétaire de l'instrument doit donner à l'autorité d'examen un libre accès au répertoire de l'instrument de manière qu'elle puisse déterminer si ce répertoire satisfait à toutes les prescriptions associées en matière de précision du mappage.

6.7 Le propriétaire de l'instrument doit permettre à l'autorité d'examen d'utiliser le répertoire pour identifier toute faille devant être ajoutée à la liste CWE.

6.8 Pour être efficace par rapport à la liste CWE, l'instrument doit être compatible avec ladite liste.

6.9 Pour être efficace par rapport à la liste CWE, le propriétaire de l'instrument doit faire parvenir à l'autorité d'examen un "formulaire d'évaluation des prescriptions en matière d'efficacité par rapport à la liste CWE" dûment rempli.

6.10 Pour être efficace par rapport à la liste CWE, le propriétaire de l'instrument doit faire parvenir à l'autorité d'examen les résultats des essais, en tant qu'élément du "formulaire d'évaluation des prescriptions en matière d'efficacité par rapport à la liste CWE", de manière qu'elle puisse déterminer si l'instrument satisfait à toutes les prescriptions associées en matière d'efficacité.

6.11 Le propriétaire de l'instrument doit accepter de se soumettre à toutes les prescriptions obligatoires en matière de compatibilité avec la liste CWE et d'efficacité par rapport à elle, y compris aux prescriptions obligatoires relatives au type particulier d'instrument.

6.12 Concernant la compatibilité CWE, l'instrument doit permettre aux utilisateurs de repérer les éléments de sécurité au moyen des identificateurs CWE ("recherche CWE").

6.13 Concernant la compatibilité CWE, lorsque l'instrument présente des éléments de sécurité à l'utilisateur, il doit lui permettre d'obtenir les identificateurs CWE associés ("sortie CWE").

6.14 Concernant la compatibilité CWE, le mappage de l'instrument doit relier les éléments de sécurité avec précision aux identificateurs CWE appropriés ("précision du mappage").

6.15 Concernant la compatibilité CWE, la documentation de l'instrument doit décrire comme il convient la liste CWE, la compatibilité CWE et la manière dont est employée dans l'instrument la fonctionnalité liée à la liste ("documentation CWE").

6.16 Concernant la compatibilité CWE, la documentation accessible au public sur l'instrument doit expressément faire état des identificateurs CWE considérés par le propriétaire de l'instrument comme étant couverts par l'instrument dans le cadre de sa fonctionnalité ("couverture CWE").

6.17 Concernant la compatibilité CWE, le site web de l'instrument accessible au public devrait fournir la couverture CWE de l'instrument sous la forme d'un ou de plusieurs document(s) en format XML représentant une déclaration de couverture CWE (CCR, *coverage claim representation*).

6.18 Concernant l'efficacité CWE, les résultats de l'évaluation par l'instrument des ensembles d'essais pour les identificateurs CWE (énumérés comme la couverture CWE de l'instrument) doivent être placés sur le site web CWE de l'autorité d'examen ("résultats d'essai CWE").

6.19 L'instrument doit indiquer la version datée de la liste CWE qui est employée ("version employée").

6.20 L'instrument doit satisfaire les prescriptions supplémentaires ci-après, applicables au type particulier d'instrument, comme spécifié à l'Annexe A.

6.21 L'instrument doit satisfaire à toutes les prescriptions applicables à ses supports de diffusion, comme spécifié à l'Annexe B.

6.22 Il n'est pas obligatoire que l'instrument:

- emploie les mêmes descriptions ou références que celles de la liste CWE;
- inclue chacun des identificateurs CWE dans son répertoire.

6.23 Si l'instrument ne satisfait pas à toutes les prescriptions applicables susmentionnées (§ 6.1 à 6.22), son propriétaire ne doit pas annoncer qu'il est conforme aux parties de la présente Recommandation concernant la compatibilité CWE ou l'efficacité CWE.

7 Précision

La compatibilité CWE ne facilite le partage et la corrélation de données que si le mappage de l'instrument est précis. En raison de cela, les instruments compatibles avec la liste CWE doivent satisfaire aux prescriptions minimales ci-après en matière de précision.

7.1 La précision du répertoire doit être de 100%.

7.2 Pendant la période d'examen, le propriétaire de l'instrument doit rectifier toutes les erreurs de mappage relevées par l'autorité d'examen.

7.3 Après la période d'examen, le propriétaire de l'instrument doit, après la signalisation d'une erreur de mappage, la rectifier dans un laps de temps raisonnable, c'est-à-dire dans un délai inférieur à la période séparant deux versions du répertoire de l'instrument ou à six mois, la plus petite de ces valeurs étant retenue.

7.4 Le propriétaire de l'instrument doit établir et signer une déclaration indiquant qu'à sa connaissance il n'y a aucune erreur dans le mappage.

7.5 Si l'instrument est fondé sur un autre instrument compatible avec la liste CWE (l'"instrument source") ou emploie celui-ci et que le propriétaire de l'instrument se rend compte que l'instrument source contient des erreurs de mappage, il doit signaler ces erreurs au propriétaire de l'instrument source.

8 Efficacité

L'objectif de l'efficacité est avant tout d'assurer la transparence de l'instrument pour les utilisateurs potentiels, afin que les failles correspondantes dans un logiciel puissent être identifiées. Les indications concernant les possibilités dont dispose un instrument pour détecter les failles en dépit des différents niveaux de complexité intéressent les utilisateurs lorsqu'ils envisagent d'employer un instrument ou de se fonder sur les résultats d'un autre utilisateur employant un instrument. En raison de cela, les instruments efficaces par rapport à la liste CWE doivent satisfaire aux prescriptions minimales ci-après en matière d'efficacité.

8.1 Le propriétaire de l'instrument doit indiquer, en employant la partie appropriée du "formulaire d'évaluation des prescriptions en matière d'efficacité par rapport à la liste CWE", les identificateurs CWE pour lesquels il déclare que l'instrument est efficace, s'agissant de la recherche. Cela peut se faire à l'aide d'un ou de plusieurs document(s) en format XML représentant la déclaration de couverture CWE (CCR).

8.2 Concernant les identificateurs CWE déclarés, le propriétaire de l'instrument doit demander les ensembles d'essais appropriés afin qu'il puisse employer l'instrument pour évaluer les ensembles d'essais pour toutes les failles correspondant aux identificateurs CWE déclarés.

8.3 Dans un laps de temps convenu, le propriétaire de l'instrument doit présenter les résultats qu'il a obtenus à partir de l'évaluation des ensembles d'essais avec son instrument.

8.4 Les résultats doivent énumérer tous les fichiers des ensembles d'essais évalués et le numéro de ligne pour chaque faille repérée au moyen de l'identificateur CWE approprié.

8.5 Le propriétaire de l'instrument doit établir et signer une déclaration acceptant de placer les résultats des essais de ses instruments sur le site web CWE.

8.6 Le propriétaire de l'instrument doit présenter un "formulaire d'évaluation des prescriptions en matière d'efficacité par rapport à la liste CWE" révisé, accompagné d'une liste mise à jour des identificateurs CWE pour lesquels il déclare que l'instrument est efficace, s'agissant de la recherche, afin de refaire les essais d'efficacité pour un ensemble différent d'identificateurs CWE. Cela peut se faire à l'aide d'un ou de plusieurs document(s) en format XML représentant la déclaration de couverture CWE (CCR) mise à jour.

9 Documentation

Les prescriptions suivantes s'appliquent à la documentation qui est fournie avec l'instrument par son propriétaire.

9.1 La documentation doit comporter une description succincte de la liste CWE et de la compatibilité avec celle-ci, pouvant reprendre mot pour mot des parties de documents placés sur le site web CWE de l'autorité d'examen.

9.2 La documentation doit décrire comment l'utilisateur peut trouver les différents éléments de sécurité dans le répertoire de l'instrument, en employant les identificateurs CWE.

9.3 La documentation doit décrire comment l'utilisateur peut obtenir les identificateurs CWE des différents éléments dans le répertoire de l'instrument.

9.4 Si la documentation comporte un index, celui-ci doit inclure des renvois à la documentation sur la liste CWE en regard du mot "CWE".

10 Version de la liste CWE employée

Les utilisateurs doivent savoir quelle version de la liste CWE est employée dans le répertoire d'un instrument, eu égard à sa mise en correspondance avec la liste CWE. Le propriétaire de l'instrument peut indiquer le mappage en vigueur en employant la version de la liste CWE ou la date à laquelle le mappage a été mis à jour.

10.1 L'instrument doit identifier la version de la liste CWE ou la date de mise à jour utilisée lors de la création ou de la mise à jour du mappage à l'aide d'au moins un des moyens suivants: consignes des modifications, listes des nouvelles caractéristiques, fichiers d'aide, etc. L'instrument est "à jour" par rapport à cette version ou à cette date de mise à jour.

10.2 Chaque nouvelle version de l'instrument doit être à jour par rapport à la version de la liste CWE qui a été publiée au maximum quatre mois avant que l'instrument ait été mis à la disposition des utilisateurs. Si un instrument ne satisfait pas à cette prescription, il est "obsolète".

10.3 Lorsqu'une nouvelle version ou une mise à jour de la liste CWE est disponible sur le site web CWE, le propriétaire de l'instrument doit annoncer aux utilisateurs et utilisateurs potentiels de l'instrument après combien de temps il mettra à jour le répertoire de l'instrument.

11 Révocation de la compatibilité avec la liste CWE

On trouvera ci-après une description des responsabilités de l'autorité d'examen en ce qui concerne la révocation de la compatibilité CWE.

11.1 Si une autorité d'examen a vérifié qu'un instrument est compatible avec une liste CWE ou est efficace par rapport à elle, mais que plus tard elle prouve que les prescriptions ne sont pas respectées, elle peut révoquer son approbation.

11.1.1 L'autorité d'examen doit identifier les prescriptions spécifiques qui ne sont pas respectées.

11.2 L'autorité d'examen doit déterminer si les actions ou les déclarations du propriétaire de l'instrument sont "intentionnellement trompeuses".

11.2.1 L'autorité d'examen peut interpréter les termes "intentionnellement trompeuses" comme elle le souhaite.

11.3 L'autorité d'examen ne devrait pas envisager de révoquer la compatibilité d'un instrument donné avec la liste CWE plus d'une fois tous les six mois.

11.4 L'autorité d'examen doit adresser au propriétaire de l'instrument et au point de contact technique un avertissement de révocation au moins deux mois avant la date prévue pour la révocation.

11.4.1 Si l'autorité d'examen constate que les actions ou les déclarations du propriétaire de l'instrument sont intentionnellement trompeuses, elle peut ne pas tenir compte de la période de préavis.

11.5 Si le propriétaire de l'instrument estime que les prescriptions sont respectées, il peut répondre à l'avertissement de révocation en fournissant des détails précis indiquant pourquoi l'instrument satisfait auxdites prescriptions.

11.6 Si le propriétaire de l'instrument modifie l'instrument au cours de la période de préavis de manière qu'il satisfasse auxdites prescriptions, l'autorité d'examen doit mettre un terme au processus de révocation pour l'instrument.

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

11.8 L'autorité d'examen doit annoncer sur le site web CWE de l'autorité d'examen que la compatibilité avec la liste CWE ou l'efficacité par rapport à elle a été révoquée pour l'instrument.

11.9 Si l'autorité d'examen estime que les actions du propriétaire de l'instrument, en ce qui concerne les prescriptions en matière de compatibilité avec la liste CWE ou d'efficacité par rapport à elle, sont intentionnellement trompeuses, la révocation doit s'étendre sur une année au minimum.

11.10 L'autorité d'examen peut rendre publics les motifs de la révocation

11.11 Le propriétaire de l'instrument peut placer une déclaration publique concernant la révocation sur le même site.

11.12 Si l'approbation est révoquée, le propriétaire de l'instrument ne doit pas se présenter pour un nouvel examen au cours de la période de révocation.

12 Autorité d'examen

12.1 Une autorité d'examen doit examiner la compatibilité avec la liste CWE et l'efficacité par rapport à elle d'un instrument, par rapport à une version donnée de la liste CWE, à savoir la version de l'examen.

12.2 Une autorité d'examen doit clairement identifier la version de l'examen qui a été employée pour déterminer la compatibilité ou l'efficacité de l'instrument.

12.3 Une autorité d'examen doit clairement identifier la version des prescriptions en matière de compatibilité avec la liste CWE et le document concernant l'efficacité qui ont été employés pour déterminer la compatibilité ou l'efficacité de l'instrument.

12.4 Une autorité d'examen doit examiner chaque élément dans le répertoire de l'instrument quant à la précision du mappage CWE.

12.5 Une autorité d'examen doit examiner la précision du mappage pour un instrument une fois par an.

Annexe A

Prescriptions selon les types d'instrument

(Cette annexe fait partie intégrante de la présente Recommandation.)

Puisqu'une gamme d'instruments très divers emploie une liste CWE, certains types d'instruments peuvent avoir des caractéristiques uniques, qui nécessitent une attention particulière en ce qui concerne la compatibilité avec la liste CWE.

A.1 L'instrument doit satisfaire à toutes les prescriptions supplémentaires qui sont liées au type particulier qui est le sien.

A.1.1 Si l'instrument est un outil d'évaluation, un analyseur de la sécurité du code source ou du code binaire, un outil d'évaluation de la qualité du code, un compilateur de vérification du code, un environnement de développement ou un produit qui intègre les résultats d'un ou de plusieurs de ces types d'éléments, il doit satisfaire aux prescriptions A.2.1 à A.2.8 relatives aux outils.

A.1.2 Si l'instrument est un service (tel qu'un service d'évaluation de la sécurité, un service d'enseignement ou de formation, ou un service d'examen du code et de la conception), il doit satisfaire aux prescriptions A.3.1 à A.3.5 relatives aux services de sécurité.

A.1.3 Si l'instrument est une base de données en ligne sur les questions de sécurité ou les failles dans un logiciel d'application, une ressource Internet ou un site d'information, il doit satisfaire aux prescriptions A.4.1 à A.4.3 relatives aux instruments en ligne.

A.2 Prescriptions relatives aux outils

Les prescriptions relatives aux outils sont les suivantes:

A.2.1 L'outil doit permettre à l'utilisateur d'employer les identificateurs CWE pour repérer les missions associées à cet outil ("recherche CWE"), en fournissant au moins l'un des éléments suivants: une fonction "recherche", un mappage entre les noms des missions de cet outil et des identificateurs CWE, ou un autre mécanisme jugé suffisant par l'autorité d'examen.

A.2.2 Pour tout rapport où sont identifiés différents éléments de sécurité, l'outil doit permettre à l'utilisateur de déterminer les identificateurs CWE associés à ces éléments ("sortie CWE"), en procédant à au moins l'une des actions suivantes: inclure les identificateurs CWE directement dans le rapport, effectuer un mappage entre les noms des missions de l'outil et les identificateurs CWE, ou employer un autre mécanisme jugé suffisant par l'autorité d'examen.

A.2.3 La documentation mise à disposition du public doit explicitement mentionner les identificateurs CWE dont le propriétaire de l'instrument estime que l'outil assure la recherche dans le logiciel ("couverture revendiquée de compatibilité avec la liste CWE").

A.2.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CWE de l'instrument sous la forme d'un ou de plusieurs document(s) en format XML représentant la déclaration de couverture CWE (CCR).

A.2.5 Tout rapport ou mappage exigé doit satisfaire aux prescriptions en matière de support, comme spécifié à l'Annexe B.

A.2.6 L'outil ou le propriétaire de l'instrument doit communiquer à l'utilisateur une liste de tous les identificateurs CWE qui sont associés aux missions de l'outil.

A.2.7 En fournissant un fichier contenant une liste des identificateurs CWE à l'utilisateur, l'outil doit permettre à celui-ci de choisir un ensemble de missions.

A.2.8 L'interface de l'outil doit permettre à l'utilisateur de naviguer, de choisir et de désélectionner un ensemble de missions au moyen des différents identificateurs CWE.

A.2.9 Si l'outil n'a aucune mission associée à un identificateur CWE, comme spécifié par l'utilisateur dans les prescriptions A.2.5 et A.2.6 relatives à l'outil, il doit informer l'utilisateur qu'il ne peut exécuter la mission associée.

A.2.10 Le propriétaire de l'instrument doit garantir 1) que le taux de faux positifs est inférieur à 100%, ce qui veut dire que le signalement par l'outil d'un élément de sécurité spécifique est parfois correct; et 2) que le taux des faux négatifs est inférieur à 100%, ce qui veut dire que l'outil signale parfois un problème, alors que celui-ci est dû à une intervention humaine dans le système, liée à un élément de sécurité spécifique.

A.3 Prescriptions relatives aux services de sécurité

Les services de sécurité peuvent employer des outils compatibles avec la liste CWE et efficaces par rapport à elle dans leurs travaux, mais ils ne peuvent donner à leurs clients un accès direct à ces outils. Il peut donc être difficile pour leurs clients de recenser et de comparer les capacités des divers services. Les prescriptions relatives aux services de sécurité traitent de cette restriction potentielle.

A.3.1 Le service de sécurité doit être en mesure d'employer des identificateurs CWE pour indiquer à un utilisateur les éléments de sécurité qui sont éprouvés, détectés ou couverts par l'offre de service ("recherche CWE"), en procédant à l'une ou à plusieurs des actions suivantes: transmettre à l'utilisateur une liste des identificateurs CWE qui recense les éléments éprouvés, détectés ou couverts par ce service, communiquer à l'utilisateur un mappage entre les éléments de service et les identificateurs CWE, répondre à une liste d'identificateurs CWE présentée par l'utilisateur, en indiquant les identificateurs CWE qui sont éprouvés, détectés ou couverts par le service ou en employant un autre mécanisme.

A.3.2 Pour tout rapport où sont identifiés différents éléments de sécurité, le service doit permettre à l'utilisateur de déterminer les identificateurs CWE associés à ces éléments ("sortie CWE"), en procédant à au moins l'une des actions suivantes: autoriser l'utilisateur à inclure les identificateurs CWE directement dans le rapport, communiquer à l'utilisateur un mappage entre les éléments de sécurité et les identificateurs CWE, ou employer un autre mécanisme.

A.3.3 La documentation mise à la disposition du public doit explicitement mentionner les identificateurs CWE dont le propriétaire de l'instrument estime que le service de sécurité assure efficacement la couverture ("couverture revendiquée de compatibilité avec la liste CWE").

A.3.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CWE de l'instrument sous la forme d'un ou de plusieurs documents en format XML représentant la déclaration de couverture CWE (CCR).

A.3.5 Tout rapport ou mappage exigé qui est fourni par le service doit satisfaire aux prescriptions en matière de support, comme spécifié à l'Annexe B.

A.3.6 Si le service donne à l'utilisateur un accès direct à un produit qui identifie les éléments de sécurité, ce produit doit être compatible avec la liste CWE et efficace par rapport à elle.

A.3.7 Le propriétaire de l'instrument doit garantir 1) que le taux de faux positifs est inférieur à 100%, ce qui veut dire que le signalement par le service d'un élément de sécurité spécifique est parfois correct; et 2) que le taux des faux négatifs est inférieur à 100%, ce qui veut dire que le service signale parfois un problème, alors que celui-ci est dû à une intervention humaine dans le système, liée à un élément de sécurité spécifique.

A.4 Prescriptions relatives aux instruments en ligne

Les prescriptions relatives aux instruments en ligne sont les suivantes:

A.4.1 L'instrument en ligne doit permettre à un utilisateur de découvrir des éléments de sécurité dans le répertoire des instruments en ligne ("recherche CWE") en fournissant l'un des éléments suivants: une fonction de recherche qui renvoie des identificateurs CWE pour les éléments associés, un mappage qui relie chaque élément avec son ou ses identificateurs CWE associés, ou un autre mécanisme.

A.4.1.1 L'instrument en ligne doit fournir un modèle d'URL qui permette à un programme d'ordinateur d'établir aisément une liaison permettant d'accéder à la fonction de recherche, comme décrit dans les prescriptions A.4.1 relatives aux instruments en ligne.

Exemples:

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

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

A.4.1.2 Si le site est accessible au public sans exiger d'identification, le programme d'identification CGI doit accepter la méthode "GET".

A.4.2 Pour tout rapport où sont identifiés différents éléments de sécurité, l'instrument en ligne doit permettre à l'utilisateur de déterminer les identificateurs CWE associés à ces éléments ("sortie CWE"), en procédant à au moins l'une des actions suivantes: autoriser l'utilisateur à inclure les identificateurs CWE directement dans le rapport, communiquer à l'utilisateur un mappage entre les éléments de sécurité et les identificateurs CWE, ou employer un autre mécanisme.

A.4.3 La documentation mise à disposition du public doit explicitement mentionner les identificateurs CWE dont le propriétaire de l'instrument estime que le répertoire de l'instrument en ligne assure efficacement la couverture ("déclaration de couverture de compatibilité avec la liste CWE").

A.4.4 Le site web de l'instrument accessible au public peut fournir la couverture revendiquée de compatibilité avec la liste CWE de l'instrument sous la forme d'un ou de plusieurs documents en format XML représentant la déclaration de couverture CWE (CCR).

A.4.5 Si l'instrument en ligne ne fournit pas les détails des différents éléments de sécurité, il doit effectuer un mappage qui relie chaque élément avec son ou ses identificateurs CWE associés.

Annexe B

Prescriptions en matière de support

(Cette annexe fait partie intégrante de la présente Recommandation.)

B.1 Le support de diffusion qui est employé par un instrument compatible avec une liste CWE doit avoir un format qui figure dans la présente annexe.

B.2 Le format du support doit satisfaire aux prescriptions propres à ce format.

B.3 Documents sous forme électronique (en format HTML, en format de traitement de texte, en format PDF, en format ASCII, etc.)

B.3.1 Le document doit avoir un format couramment disponible, disposant de lecteurs qui prennent en charge la fonction "recherche" ("recherche CWE"), tel que le format texte ASCII brut, le format HTML ou le format PDF.

B.3.2 Si le document ne fournit que des abréviations ou des titres pour les différents éléments, il doit énumérer les identificateurs CWE qui sont reliés à ces éléments ("sortie CWE").

B.3.3 Le document doit inclure un mappage entre les éléments et les identificateurs CWE, où sont énumérés les pages appropriées pour chaque élément.

B.4 Interface graphique utilisateur (GUI)

Les prescriptions relatives à l'interface graphique utilisateur sont les suivantes:

B.4.1 L'interface GUI doit fournir à l'utilisateur une fonction de recherche qui permette à l'utilisateur d'introduire un identificateur CWE et d'extraire les éléments correspondants ("recherche CWE").

B.4.2 Lorsque l'interface GUI énumère les détails d'un élément, elle doit énumérer les identificateurs CWE qui correspondent à cet élément ("sortie CWE"). Sinon, elle doit mettre à la disposition de l'utilisateur un mappage sous un format qui satisfait à la prescription B.3.1 relative aux documents sous forme électronique.

B.4.3 L'interface GUI doit permettre à l'utilisateur d'exporter des données se rapportant à la liste CWE ou d'y accéder, sous un autre format, à condition que celui-ci satisfasse à la prescription B.3.1 relative aux documents sous forme électronique.

Appendice I

Liste des répertoires d'identificateurs CWE et des informations corollaires associées

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

MITRE Corporation	cwe.mitre.org/data

Appendice II

Liste des autorités d'examen

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

1) MITRE Corporation, à contacter via cwe@mitre.org.

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, 2012