Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1520

(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

Vulnérabilités et expositions courantes

Recommandation UIT-T X.1520

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.1520

Vulnérabilités et expositions courantes

Résumé

La Recommandation UIT-T X.1520 relative à l'utilisation des vulnérabilités et expositions courantes (CVE, *common vulnerabilities and exposures*) traite d'un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions courantes en matière de sécurité de l'information, qui fournit des dénominations communes pour les problèmes connus du public rencontrés dans les logiciels commerciaux ou libres utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final, ou dans tout autre type de dispositif des technologies de l'information et de la communication (TIC) utilisant des logiciels. La présente Recommandation vise à définir l'utilisation des CVE pour faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services) sur la base de ces dénominations communes. Elle définit l'utilisation des CVE en vue d'offrir un mécanisme pour permettre d'utiliser en association des bases de données sur les vulnérabilités et d'autres capacités, d'une part, et de faciliter la comparaison des outils et services de sécurité, d'autre part. Cette Recommandation ne prend pas en considération les informations telles que des informations sur les risques, les incidences et les solutions, ou des informations techniques détaillées. Elle prend uniquement en considération le numéro d'identification standard avec un indicateur d'état, une brève description, et des références aux rapports et avis de vulnérabilité associés. Le répertoire des identifiants de CVE est disponible à l'adresse cve.mitre.org/cve/cve.html.

Le but des CVE, dont l'utilisation est définie dans la présente Recommandation, est de pouvoir identifier toutes les vulnérabilités et expositions connues du public. Cette Recommandation est conçue pour prendre en considération des informations bien établies, mais l'objectif premier est d'identifier les vulnérabilités et les expositions qui sont détectées par les outils de sécurité ainsi que tout nouveau problème rendu public, puis de régler les éventuels problèmes de sécurité plus anciens qui nécessitent une validation.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
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

* 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/.

© UIT 2014

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

Introduction

La présente Recommandation relative à l'utilisation des vulnérabilités et expositions courantes (CVE, *common vulnerabilities and exposures*) traite d'un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions courantes en matière de sécurité de l'information, qui fournit des dénominations communes pour les problèmes connus du public. La présente Recommandation vise à définir l'utilisation des CVE pour faciliter l'échange de données sur les vulnérabilités entre différentes capacités (outils, répertoires et services) sur la base de ces dénominations communes. Elle est conçue pour permettre d'utiliser en association des bases de données sur les vulnérabilités et d'autres capacités, et pour faciliter la comparaison des outils et services de sécurité. La présente Recommandation ne prend pas en considération les informations telles que des informations sur les risques, les incidences et les solutions, ou des informations techniques détaillées. Elle prend uniquement en considération le numéro d'identification standard avec un indicateur d'état, une brève description, et des références aux rapports et avis de vulnérabilité associés. Le répertoire des identifiants de CVE est disponible à l'adresse cve.mitre.org/cve/cve.html.

Le but des CVE, dont l'utilisation est définie dans la présente Recommandation, est de pouvoir identifier toutes les vulnérabilités et expositions connues du public. La présente Recommandation est conçue pour prendre en considération des informations bien établies, mais l'objectif premier est d'identifier les vulnérabilités et les expositions qui sont détectées par les outils de sécurité ainsi que tout nouveau problème rendu public, puis de régler les éventuels problèmes de sécurité plus anciens qui nécessitent une validation.

La présente Recommandation fait partie d'un ensemble de Recommandations de l'UIT-T provenant d'une vaste communauté de développement et d'utilisateurs existant dans le monde, qui a rédigé et fait évoluer une spécification ouverte mise à la disposition de l'UIT-T à des fins d'adoption, étant entendu que toute modification ou mise à jour des spécifications sera réalisée de manière à veiller à ce que l'équivalence et la compatibilité techniques soient pleinement maintenue, que les discussions concernant les modifications et améliorations auront lieu au sein de la communauté d'utilisateurs d'origine et qu'elle inclut une référence explicite à la version spécifique correspondante maintenue par la communauté d'utilisateurs.

Recommandation UIT-T X.1520

Vulnérabilités et expositions courantes

1 Domaine d'application

La présente Recommandation relative à l'utilisation des vulnérabilités et expositions courantes traite d'un "moyen structuré" d'échanger sur le plan mondial des informations sur les vulnérabilités et les expositions matures connues du public qui sont détectées par les outils de sécurité ou rendues publiques d'une autre manière. Ce "moyen structuré" est souvent appelé "compatibilité CVE" et définit la bonne utilisation des CVE. Une vulnérabilité en matière de sécurité de l'information est une erreur de logiciel pouvant être directement utilisée par un pirate pour accéder à un système ou réseau. Une exposition en matière de sécurité de l'information est une erreur de logiciel qui permet d'accéder à des informations ou capacités pouvant être utilisées par un pirate comme tremplin pour accéder à un système ou réseau. L'attribution des identifiants de CVE n'entre pas dans le domaine d'application de la présente Recommandation.

La Recommandation UIT-T X.1520 a été élaborée en collaboration avec la société MITRE, compte tenu du fait qu'il était important de maintenir, dans la mesure du possible, la compatibilité sur le plan technique avec le document "*Requirements and Recommendations for CVE Compatibility*", daté du 30 juin 2013, disponible à l'adresse:
https://cve.mitre.org/compatible/Requirements_for_CVE_Compatibility_V1.3.pdf.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 pourcentage d'exactitude: Il s'agit du pourcentage d'éléments de sécurité dans l'échantillon d'examen référençant les bons identifiants de CVE.

3.2.2 capacité: outil de sécurité, base de données, site web, conseil ou service fournissant une fonction d'identification d'une vulnérabilité ou d'une exposition de sécurité.

3.2.3 exposition: exposition à un problème de sécurité de l'information qui est une erreur de logiciel pouvant être directement utilisée par un pirate pour accéder à un système ou réseau.

3.2.4 mise en correspondance/mappage: spécification des relations entre les éléments de sécurité d'un répertoire et les noms de CVE liés à ces éléments.

3.2.5 propriétaire: détenteur (personne ou entreprise) qui est responsable de la capacité.

3.2.6 répertoire: recueil implicite ou explicite des éléments de sécurité prenant en charge une capacité, par exemple une base de données de vulnérabilités, une archive de conseils, l'ensemble des signatures dans un système de détection d'intrusion (IDS, *intrusion detection system*) ou site web.

3.2.7 examen: processus de détermination de la compatibilité CVE d'une capacité.

3.2.8 autorité d'examen: entité qui réalise un examen.

NOTE – MITRE est actuellement la seule autorité d'examen.

3.2.9 date d'examen: date du contenu CVE qui est utilisée pour déterminer la compatibilité CVE d'une capacité.

3.2.10 échantillon d'examen: ensemble des éléments de sécurité dans le répertoire de la capacité, qui est utilisé par l'autorité d'examen pour l'évaluation de l'exactitude.

3.2.11 méthode d'échantillonnage: méthode suivant laquelle l'autorité d'examen identifie l'ensemble des éléments de sécurité dans l'échantillon d'examen.

3.2.12 taille de l'échantillon: pourcentage et/ou du nombre d'éléments de sécurité que l'autorité d'examen doit examiner.

3.2.13 élément de sécurité: enregistrement dans une base de données, courrier électronique, alerte de sécurité, sonde d'évaluation, signature, etc., en relation avec une vulnérabilité ou exposition donné.

3.2.14 tâche: sonde, vérification, signature, etc., d'un outil, qui réalise une action fournissant des informations de sécurité (c'est-à-dire l'élément de sécurité).

3.2.15 outil: application logicielle ou équipement qui examine un serveur ou un réseau et fournit des informations en relation avec les vulnérabilités et expositions, ou agrège ce type d'informations (par exemple, scanner de vulnérabilités, système de détection d'intrusion, gestion des risques, gestion d'informations de sécurité, ou outil ou service de notification de conformité).

3.2.16 utilisateur: un consommateur ou consommateur potentiel de la capacité.

3.2.17 vulnérabilité: faiblesse d'un logiciel susceptible d'être exploitée pour violer un système ou les informations qu'il contient (sur la base de [b-UIT-T X.1500]).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASCII code américain normalisé pour l'échange d'information (*American Standard Code for Information Interchange*

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

GUI interface graphique (*graphical user interface*)

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

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

IDS système de détection d'intrusion (*intrusion detection system*)

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

POC point de contact (*point of contact*)

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

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

5 Conventions

L'abréviation CVE est utilisée comme un substantif dans la présente Recommandation.

6 Prescriptions de haut niveau

Les éléments ci-après définissant les concepts, les rôles et les responsabilités concernant la bonne utilisation des identifiants de CVE pour que des capacités distinctes (outils, répertoires et services) puissent échanger des données afin de permettre d'utiliser en association des bases de données sur les vulnérabilités et d'autres capacités et de faciliter la comparaison des outils et services de sécurité.

Conditions préalables

6.1 Le propriétaire de la capacité est une entité juridique (organisation ou individu spécifique) avec un numéro de téléphone, une adresse électronique et une adresse postale valides.

6.2 La capacité fournit des valeurs ou informations supplémentaires en plus de celles fournies par le CVE lui-même (nom, description, références et données associées).

6.3 Le propriétaire de la capacité fournit à l'autorité d'examen un point de contact technique compétent pour répondre aux questions en rapport avec le mappage et les fonctionnalités de la capacité en relation avec le CVE.

6.4 La capacité est disponible pour le public ou un ensemble de consommateurs, dans une version de production.

6.5 Le propriétaire de la capacité fournit à l'autorité d'examen un "formulaire d'évaluation des prescriptions de compatibilité CVE" rempli.

6.6 Dans le cas d'une capacité dotée d'un répertoire, le propriétaire fournit à l'autorité d'examen l'accès libre au répertoire afin de permettre à l'autorité de déterminer si le répertoire satisfait toutes les prescriptions associées.

6.7 Dans le cas d'une capacité dotée d'un répertoire, le propriétaire de la capacité permet à l'autorité d'examen d'utiliser le répertoire pour identifier toute vulnérabilité qui devrait être ajoutée au CVE.

6.8 Le propriétaire de la capacité s'engage à respecter toutes les prescriptions de compatibilité CVE obligatoires, y compris les prescriptions obligatoires pour le type spécifique de capacité.

Fonctionnalité

6.9 La capacité permet aux utilisateurs de localiser les éléments de sécurité à l'aide de noms de CVE ("*CVE-searchable*").

6.10 Lorsque la capacité présente des éléments de sécurité à l'utilisateur, elle permet à l'utilisateur d'obtenir les noms de CVE associés ("*CVE-output*").

6.11 Dans le cas d'une capacité dotée d'un répertoire, le mappage de la capacité lie de manière exacte les éléments de sécurité aux noms de CVE appropriés ("*mapping accuracy*").

6.12 La documentation de la capacité décrit de manière adéquate les CVE, la compatibilité CVE et la manière dont la fonctionnalité en relation avec le CVE dans la capacité est utilisée ("*CVE-documentation*").

6.13 La capacité déclare la date à laquelle elle a été établie par rapport au CVE ("*date usage*").

6.14 La capacité respecte toute prescription supplémentaire pour le type spécifique de capacité, comme spécifié dans l'Annexe A.

6.15 La capacité satisfait toutes les prescriptions applicables à son support de distribution, comme spécifié dans l'Annexe B.

6.16 Il n'est pas nécessaire que la capacité:

- utilise les mêmes descriptions ou références que les CVE;
- intègre tous les noms de CVE dans son répertoire.

Divers

6.17 Si la capacité ne satisfait pas toutes les prescriptions applicables susmentionnées (§ 6.1 à 6.16), le Propriétaire de la capacité n'annonce pas qu'elle est compatible CVE.

7 Exactitude

La compatibilité CVE ne peut faciliter le partage de données que si le mappage de la capacité est exact. C'est pourquoi les capacités compatibles CVE doivent satisfaire les prescriptions minimales d'exactitude décrites ci-après.

7.1 Dans le cas d'une capacité dotée d'un répertoire, le répertoire a un pourcentage d'exactitude d'au moins 90%.

7.2 Au cours d'une période d'examen, le propriétaire de la capacité corrige toutes les erreurs de mappage trouvées par l'autorité d'examen.

7.3 Après la période d'examen, le propriétaire de la capacité devrait corriger une erreur de mappage dans un délai raisonnable après que l'erreur a été initialement rapportée, c'est-à-dire dans un délai correspondant à deux (2) versions du répertoire ou six (6) mois pour les outils et trois (3) mois pour les capacités et services en ligne.

7.4 Dans le cas d'une capacité dotée d'un répertoire, le propriétaire de la capacité devrait préparer et signer une déclaration stipulant qu'à sa connaissance, il n'y a pas d'erreur dans le mappage.

7.5 Si la capacité est basée sur une autre capacité compatible CVE (la capacité "source") ou utilise une telle capacité et que son propriétaire se rend compte qu'il existe des erreurs de mappage dans la capacité source, alors le propriétaire de la capacité rapporte ces erreurs au propriétaire de la capacité source.

7.6 L'exactitude du mappage pour les archives de conseils est évaluée par rapport à tous les éléments de sécurité du répertoire d'archive correspondant à la première utilisation par l'archive d'un nom de CVE dans un élément de sécurité et des répertoires suivants.

7.7 Une capacité rend compte avec exactitude du statut des noms de CVE obsolètes dans un délai de trois (3) mois pour les capacités et les services en ligne.

7.8 Une capacité ne produit pas d'identifiants de CVE obsolètes lorsque des identifiants plus adaptés figurent dans la description de l'identifiant de CVE obsolète, dans un délai de trois (3) mois après que l'identifiant en question est devenu obsolète.

8 Documentation

Les prescriptions suivantes s'appliquent à la documentation fournie avec la capacité.

8.1 La documentation inclut une description concise du CVE et de la compatibilité CVE, pouvant se baser sur des portions verbatim de documents du site web du CVE.

8.2 La documentation décrit comment l'utilisateur peut trouver des éléments de sécurité particuliers dans le répertoire d'une capacité à l'aide de noms de CVE.

8.3 La documentation décrit comment l'utilisateur peut obtenir des noms de CVE à partir d'éléments particuliers dans le répertoire de la capacité.

8.4 Si la documentation comprend un index, alors il devrait inclure les références à la documentation en relation avec le CVE sous le terme "CVE".

9 Utilisation de la date des CVE

Les utilisateurs doivent pouvoir déterminer dans quelle mesure le répertoire d'une capacité est "à jour" eu égard à son mappage avec les CVE. Le propriétaire de la capacité doit indiquer cette information en donnant la date de la dernière mise à jour des informations de CVE et en indiquant quelle part du contenu de CVE il a utilisée, ainsi que la provenance de ce contenu.

9.1 Chaque nouvelle version de la capacité identifie la date la plus récente du contenu CVE utilisé pour la création ou la mise à jour du mappage grâce à au moins l'un des éléments suivants: journal log des modifications, liste des nouvelles fonctionnalités, fichiers d'aide, ou en utilisant un autre mécanisme. La capacité est "à jour" eu égard à cette date.

9.2 Chaque nouvelle version de la capacité est à jour eu égard à la date des CVE indiquée qui n'est pas antérieure de trois (3) mois à la date à laquelle la capacité a été mise à la disposition de ses utilisateurs. Si une capacité ne satisfait pas cette prescription, elle est alors "obsolète".

9.3 Le propriétaire de la capacité doit indiquer quand il mettra à jour le répertoire de la capacité afin d'inclure les nouvelles informations de CVE.

9.4 Le propriétaire de la capacité décrit les critères et mécanismes de sélection des informations de CVE qu'il va inclure dans sa capacité.

9.5 Le propriétaire de la capacité décrit d'où provient le nouveau contenu de CVE.

10 Prise en charge des différents types de noms de CVE

Une capacité fonctionne avec des noms de CVE indépendants du format de représentation des noms CVE dans la capacité, qu'elle utilise l'ancienne syntaxe des identifiants de CVE à quatre chiffres ou la syntaxe à longueur variable (quatre chiffres ou plus) qui sera utilisée après la modification, le 30 décembre 2013, de la syntaxe des identifiants de CVE en vigueur.

10.1 Si un utilisateur effectue une recherche à l'aide de YYYY-NNNN, de YYYY-NNNNN, YYYY-NNNNNN ou d'autres identifiants valides comprenant un grand nombre de chiffres, la capacité renvoie les éléments de sécurité correspondant respectivement à CVE-YYYY-NNNN, à CVE-YYYY-NNNNN, à CVE-YYYY-NNNNNN ou à d'autres identifiants valides comprenant un grand nombre de chiffres, peu importe que le nom de CVE ait un CVE ou un CAN comme partie de son nom, au sein du répertoire de la capacité.

10.2 Si la capacité contient le nom CVE CVE-YYYY-NNNN, mais que l'utilisateur fait une recherche à l'aide de l'ancien format de noms CVE, CAN-YYYY-NNNN (utilisé avant la modification du schéma de nommage des CVE introduite le 19 octobre 2005), alors la capacité devrait renvoyer CVE-YYYY-NNNN.

11 Révocation de la compatibilité de CVE

11.1 Si une autorité d'examen a vérifié qu'une capacité est compatible CVE, mais qu'elle a par la suite la preuve que les prescriptions ne sont plus satisfaites, elle peut alors révoquer son approbation.

11.1.1 L'autorité d'examen identifie les prescriptions spécifiques qui ne sont pas satisfaites.

11.2 L'autorité d'examen détermine si les actions ou déclarations du propriétaire de la capacité sont "intentionnellement trompeuses".

11.2.1 L'autorité d'examen peut interpréter la phrase "intentionnellement trompeuse" comme elle le souhaite.

11.3 Sauf recommandation par deux membres du Comité de rédaction de CVE n'ayant pas de conflit d'intérêt, l'autorité d'examen ne devrait pas envisager plus d'une fois tous les six (6) mois la révocation d'une compatibilité CVE pour une capacité donnée.

Mise en garde et évaluation

11.4 L'autorité d'examen fournit au propriétaire de la capacité et au point de contact technique (POC) un avis de révocation au moins deux (2) mois avant la date prévue pour la révocation.

11.4.1 Si elle a trouvé que les actions ou déclarations du propriétaire de la capacité étaient intentionnellement trompeuses, l'autorité d'examen peut sauter la période de préavis.

11.5 S'il pense que les prescriptions sont respectées, le propriétaire de la capacité pense satisfaire les prescriptions, alors le Propriétaire peut répondre à l'avis de révocation en fournissant les détails spécifiques indiquant pourquoi la capacité satisfait aux prescriptions en question.

11.6 Si propriétaire de la capacité modifie la Capacité de manière à la rendre conforme aux prescriptions en question pendant la période de préavis, l'autorité d'examen devrait mettre un terme à l'action de révocation de la capacité.

Révocation

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

11.8 L'autorité d'examen fait savoir que la compatibilité CVE a été révoquée pour la capacité.

11.9 Si l'autorité d'examen découvre que les actions du propriétaire de la capacité eu égard aux prescriptions de compatibilité CVE sont intentionnellement trompeuses, la révocation devrait être d'au minimum un an.

11.10 L'autorité d'examen peut faire connaître la raison de la révocation.

11.11 Si l'approbation est révoquée, le propriétaire de la capacité ne doit pas demander un nouvel examen pendant la période de révocation.

12 Autorité d'examen

Pour tout examen réalisé par l'autorité d'examen:

12.1 L'autorité d'examen examine la compatibilité CVE de la capacité eu égard à une date de contenu de CVE donné, qui est la date d'examen.

12.2 L'autorité d'examen identifie clairement la date d'examen utilisée pour déterminer la compatibilité de la capacité.

12.3 L'autorité d'examen identifie clairement la version du document des prescriptions de compatibilité CVE utilisée pour déterminer la compatibilité de la capacité.

12.4 L'autorité d'examen définit et publie une taille d'échantillon.

12.4.1 L'autorité d'examen devrait utiliser une taille d'échantillon de 50 éléments plus 5% du répertoire de la capacité, l'échantillon ne devant pas comprendre plus 400 éléments.

12.4.2 L'autorité d'examen peut examiner tous les éléments du répertoire de la capacité.

12.5 L'autorité d'examen doit faire connaître la méthode d'échantillonnage.

12.6 L'autorité d'examen peut utiliser un échantillon d'examen qui n'a pas été sélectionné de manière aléatoire.

12.7 L'autorité d'examen utilise les mêmes méthodes d'échantillonnage et taille d'échantillon pour toutes les capacités évaluées pendant la même période de temps.

Annexe A

Prescriptions spécifiques au type

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

Comme une grande variété de capacités utilise les CVE, certains types de capacités peuvent avoir des fonctionnalités uniques, qui requièrent une attention particulière eu égard à la compatibilité CVE.

A.1 La capacité satisfait toutes les prescriptions supplémentaires en relation avec le type spécifique de capacité.

A.1.1 Si la capacité est un scanner d'évaluation de vulnérabilité, un système de détection d'intrusion (IDS, *intrusion detection system*) ou un produit qui intègre les résultats d'un ou plusieurs scanners et IDS, elle doit satisfaire aux prescriptions applicables aux outils (§ A.2.1-A.2.8).

A.1.2 Si la capacité est un service (tel qu'un service géré de détection et de réponse à une intrusion, ou un service d'exploration à distance), elle satisfait aux prescriptions applicables aux services de sécurité (§ A.3.1-A.3.5).

A.1.3 Si la capacité est une base de données de vulnérabilités ou de signatures en ligne, une archive basée web, ou un site de maintenance/correctifs, elle satisfait aux prescriptions applicables aux capacités en ligne (§ A.4.1-A.4.3).

A.1.4 Si la capacité est un outil d'agrégation tel qu'un gestionnaire d'informations de sécurité, un outil de notification de conformité ou un service fournissant ce type d'agrégation des informations sur le type de vulnérabilité, elle satisfait aux prescriptions applicables aux capacités d'agrégation (§ A.5.1-A.5.6).

Prescriptions applicables aux outils

A.2.1 L'outil permet à l'utilisateur d'utiliser les noms de CVE pour localiser les tâches associées dans cet outil ("*CVE-searchable*") en effectuant au moins l'une des actions suivantes: une fonction "trouver" ou "rechercher", un mappage entre les noms des tâches de l'outil et les noms de CVE, ou en utilisant un autre mécanisme.

A.2.2 Pour tout rapport qui identifie des éléments de sécurité particuliers, l'outil permet à l'utilisateur de déterminer les noms de CVE associés à ces éléments ("*CVE-output*") en réalisant au moins l'une des actions suivantes: inclure les noms de CVE directement dans le rapport, fournir un mappage entre les noms des tâches de l'outil et les noms de CVE, ou en utilisant un autre mécanisme.

A.2.3 Tout rapport ou mappage requis satisfait les prescriptions applicables aux supports indiqués dans l'Annexe B.

A.2.4 L'outil, ou le propriétaire de la capacité, devrait fournir à l'utilisateur une liste de tous les noms de CVE qui sont associés aux tâches de l'outil.

A.2.5 L'outil devrait permettre à l'utilisateur de sélectionner un ensemble de tâches en fournissant un fichier contenant une liste des noms de CVE.

A.2.6 L'interface de l'outil devrait permettre à l'utilisateur de parcourir, de sélectionner et de désélectionner un ensemble de tâches en utilisant les différents noms de CVE.

A.2.7 Si l'outil n'a pas de tâche associée au nom de CVE comme spécifié par l'utilisateur dans les prescriptions applicables aux outils (§ A.2.5 ou A.2.6) l'outil devrait indiquer à l'utilisateur qu'il ne peut pas réaliser la tâche associée.

A.2.8 Le propriétaire de la capacité garanti que: 1) le taux de faux positifs est inférieur à 100% (si l'outil signale un élément de sécurité spécifique, il est au moins parfois correct); et 2) le taux de faux négatifs est inférieur à 100% (si un événement se produit en relation avec un élément de sécurité spécifique, l'outil rapporte parfois cet événement).

Prescriptions applicables aux services de sécurité

Les services de sécurité peuvent utiliser des outils compatibles CVE au cours de leur travail, mais ils ne fournissent pas toujours à leurs clients l'accès direct à ces outils. Il pourrait donc être difficile pour les clients d'identifier et de comparer les capacités de différents services. Les prescriptions applicables aux services de sécurité permettent de remédier à cette limite potentielle.

A.3.1 Le service de sécurité est en mesure d'utiliser les noms de CVE pour indiquer à un utilisateur quels éléments de sécurité ont été testés ou détectés par le service ("*CVE-searchable*") en réalisant au moins l'une des actions suivantes: fournir à l'utilisateur une liste des noms de CVE qui identifient les éléments qui ont été testés ou détectés par ce service, fournir à l'utilisateur un mappage entre les éléments du service et les noms de CVE, répondre à une liste fournie par un utilisateur de noms de CVE en identifiant quels sont les noms de CVE testés ou détectés par le service, ou en utilisant un autre mécanisme.

A.3.2 Pour tout rapport qui identifie des éléments de sécurité individuels, le service permet à l'utilisateur de déterminer les noms de CVE associés à ces éléments ("*CVE-output*") en réalisant au moins l'une des actions suivantes: permettre à l'utilisateur d'inclure des noms de CVE directement dans le rapport, fournir à l'utilisateur un mappage entre les éléments de sécurité et les noms de CVE, ou en utilisant un autre mécanisme.

A.3.3 Tout rapport ou mappage requis fourni par le service satisfait les prescriptions applicables aux supports définies dans l'Annexe B.

A.3.4 Si le service fournit à l'utilisateur un accès direct à un produit qui identifie des éléments de sécurité, ce produit devrait être compatible CVE.

A.3.5 Le propriétaire de la capacité garantit que: 1) le taux de faux positifs est inférieur à 100% (si l'outil signale un élément de sécurité spécifique, il est au moins parfois correct); et 2) le taux de faux négatifs est inférieur à 100% (si un événement se produit en relation avec un élément de sécurité spécifique, le service rapporte parfois cet événement).

Prescriptions applicables aux capacités en ligne

A.4.1 La capacité en ligne permet à l'utilisateur de trouver les éléments de sécurité connexes à partir du répertoire de la capacité en ligne ("*CVE-searchable*") en effectuant l'une des actions suivantes: une fonction de recherche qui renvoie les noms CVE des éléments connexes, un mappage qui lie chaque élément avec son (ou ses) nom(s) de CVE associé(s), ou en utilisant un autre mécanisme.

A.4.1.1 La capacité en ligne devrait fournir un modèle d'URL permettant à un programme informatique de construire facilement un lien pour accéder à la fonction de recherche, comme indiqué au § A.4.1, sous le titre "Prescriptions applicables aux capacités en ligne".

Exemples:
```
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
http://www.example.com/cve/CVE-YYYY-NNNNN.html
http://www.example.com/cve/CVE-YYYY-NNNNNN.html
```

A.4.1.2 Si le modèle d'URL est destiné à un programme CGI, le programme devrait accepter la méthode "GET" HTTP.

A.4.2 Pour tout rapport qui identifie des éléments de sécurité individuels, la capacité en ligne permet à l'utilisateur de déterminer les noms de CVE associés à ces éléments ("*CVE-output*") en réalisant au moins l'une des actions suivantes: permettre à l'utilisateur d'inclure des noms de CVE directement dans le rapport, fournir à l'utilisateur un mappage entre les éléments de sécurité et les noms de CVE, ou en utilisant un autre mécanisme.

A.4.3 Si la capacité en ligne ne fournit pas de détails concernant les différents éléments de sécurité, la capacité en ligne fournit un mappage qui lie chaque élément à son (ou ses) nom(s) de CVE associé(s).

Prescriptions applicables aux capacités d'agrégation

A.5.1 La capacité d'agrégation permet à l'utilisateur d'utiliser les noms de CVE pour localiser les éléments associés dans cette capacité ("*CVE-searchable*") en réalisant au moins l'une des actions suivantes: une fonction de recherche, un mappage qui lie les noms des capacités et les noms de CVE, ou en utilisant un autre mécanisme avec l'approbation de l'autorité d'examen.

A.5.2 Pour tout rapport qui identifie des éléments de sécurité individuels, la capacité d'agrégation permet à l'utilisateur de déterminer les noms de CVE associés à ces éléments ("*CVE-output*") en réalisant au moins l'une des actions suivantes: inclure des noms de CVE directement dans le rapport, fournir un mappage entre les noms de la capacité et les noms de CVE, ou en utilisant un autre mécanisme.

A.5.3 Tout rapport ou mappage requis satisfait les prescriptions applicables aux supports définies dans l'Annexe B.

A.5.4 L'outil, ou le propriétaire de la capacité, devrait fournir à l'utilisateur une liste de tous les noms de CVE qui sont associés aux tâches de l'outil.

A.5.5 L'outil devrait permettre à l'utilisateur de sélectionner un ensemble de tâches en fournissant un fichier contenant une liste des noms de CVE.

A.5.6 L'interface de l'outil devrait permettre à l'utilisateur de parcourir, de sélectionner et de désélectionner un ensemble de tâches en utilisant les différents noms de CVE.

Annexe B

Prescriptions applicables aux supports

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

B.1 Le support de distribution utilisé par une capacité compatible CVE utilise un format couvert par la présente annexe.

B.2 Le format du support satisfait les prescriptions spécifiques applicables à ce format.

Documents électroniques (HTML, traitement de texte, PDF, texte ASCII, etc.)

B.3.1 Le document est disponible dans un format usuel pour lequel le système de lecture prend en charge la fonction "trouver" ou "rechercher" ("*CVE-searchable*"), tel que le texte brut en ASCII, HTML ou PDF.

B.3.2 Si le document ne contient que des noms courts ou titres pour les différents éléments, il doit lister les noms de CVE en relation avec ces éléments ("*CVE-output*").

B.3.3 Le document devrait inclure un mappage des éléments avec les noms de CVE, qui donne les pages idoines pour chaque élément.

Interface utilisateur graphique (GUI, *Graphical user interface*)

B.4.1 La fonction de recherche de l'interface qui permet à l'utilisateur de saisir un nom de CVE et d'extraire les éléments connexes ("*CVE-searchable*").

B.4.2 Si l'interface GUI donne des détails pour un élément particulier, elle donne le (ou les) nom(s) de CVE qui corresponde(nt) à cet élément ("*CVE-output*"). Si tel n'est pas le cas, l'interface GUI fournit à l'utilisateur le mappage dans un format qui satisfait la prescription B.3.1 applicable aux documents électroniques.

B.4.3 L'interface GUI devrait permettre à l'utilisateur d'exporter des données en relation avec les CVE, ou d'y accéder, dans un autre format qui satisfait la prescription B.3.1 applicable aux documents électroniques.

Annexe C

Prescriptions applicables aux supports

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

Le schéma XML des CVE figurant dans la présente annexe est disponible à l'adresse: http://cve.mitre.org/schema/cve/cve_1.0.xsd et est reproduit ci-dessous.

```
<?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>
```

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

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