Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1525

(04/2015)

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

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

Système commun de notation des failles

Recommandation UIT-T X.1525

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
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
COMMUNICATION QUANTIQUE	X.1700–X.1729

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

Recommandation UIT-T X.1525

Système commun de notation des failles

Résumé

La Recommandation UIT-T X.1525, relative au système commun de notation des failles (CWSS, *common weakness scoring system*), définit un cadre ouvert pour la communication des caractéristiques et des incidences des failles en matière de technologies de l'information et de la communication (TIC) rencontrées au moment du développement des fonctionnalités des logiciels. L'objectif de cette Recommandation est de permettre aux concepteurs de logiciels, aux gestionnaires, aux testeurs, aux fournisseurs de systèmes de sécurité et aux prestataires de services, aux acheteurs, aux fournisseurs d'applications et aux chercheurs dans le domaine des TIC d'utiliser un langage commun en ce qui concerne la notation des failles en matière de TIC qui pourraient se traduire par des vulnérabilités au moment de l'utilisation des logiciels.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1525	17-04-2015	17	11.1002/1000/12357

* 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 on 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

Les concepteurs de logiciels sont souvent confrontés à des centaines voire des milliers de rapports de bogue différents liés à des failles découvertes dans leur code. Dans certains cas, une faille dans un logiciel peut mener jusqu'à une vulnérabilité exploitable. En raison de ce grand volume de failles signalées, les parties prenantes sont souvent amenées à prioriser les problèmes afin d'examiner et de régler en premier les problèmes prioritaires. En d'autres termes, elles doivent être en mesure de juger de l'importance relative des différentes failles et de communiquer à ce sujet. A l'heure actuelle, diverses méthodes de notation sont utilisées, mais soit elles ne s'appliquent qu'au cas par cas soit leur application est inappropriée compte tenu de l'évaluation toujours imprécise de la sécurité des logiciels. Le système commun de notation des failles (CWSS) offre un mécanisme permettant de prioriser les failles dans les logiciels de manière cohérente, souple et ouverte tout en tenant compte du contexte concernant les divers domaines d'activité et usages prévus des logiciels. C'est le fruit d'un travail de collaboration mené au sein d'une communauté visant à répondre aux besoins de ses parties prenantes dans le secteur public, les milieux universitaires et le secteur privé.

Les concepteurs de logiciels, gestionnaires, testeurs, fournisseurs de systèmes de sécurité et prestataires de services, acheteurs, fournisseurs d'applications et chercheurs dans le domaine des TIC doivent identifier et évaluer les failles dans les logiciels qui pourraient se traduire par des vulnérabilités au moment de l'utilisation des logiciels. Ils doivent ensuite pouvoir prioriser ces failles et déterminer celles qui présentent les plus grands risques afin d'y remédier. Lorsqu'il faut remédier à un grand nombre de failles, chacune étant notée sur des échelles différentes, les divers membres de la communauté des TIC, gestionnaires, testeurs, acheteurs et concepteurs, s'en remettent à leurs propres méthodologies pour trouver des moyens de comparer des failles disparates et de les traduire en informations décisionnelles.

Du fait que le système CWSS offre une approche normalisée pour la caractérisation des failles, les utilisateurs de ce système peuvent invoquer des métriques environnementales et de surface d'attaque pour appliquer des informations contextuelles qui reflètent de manière plus précise le risque pour les logiciels compte tenu du contexte d'activité particulier dans lequel ils fonctionneront et des fonctionnalités particulières qu'ils sont censés assurer. Les utilisateurs peuvent ainsi prendre des décisions plus éclairées lorsqu'ils essayent d'atténuer les risques posés par les failles.

Le système CWSS tire parti des résultats des travaux menés au sein de la communauté de la cybersécurité, notamment le grand nombre de vulnérabilités diverses connues du public rencontrées dans la pratique, qui sont spécifiées dans [b-UIT-T X.1520] – Vulnérabilités et expositions courantes – et le système de notation utilisé pour examiner la gravité de ces vulnérabilités connues du public, qui est spécifié dans [b-UIT-T X.1521] – Système d'évaluation des vulnérabilités courantes – ainsi que l'énumération des failles courantes, qui est une liste de failles rencontrées dans l'architecture, la conception, le code ou le déploiement des logiciels. Pour l'élaboration du système CWSS, il est nécessaire de pouvoir définir des valeurs par défaut raisonnables pour des domaines qui ne sont peut-être pas connus, tout en permettant une adaptation en fonction des activités et du contexte technique.

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 de la spécification sera réalisée de manière à veiller à ce que l'équivalence et la compatibilité techniques soient pleinement maintenues, que les discussions concernant les modifications et améliorations auront lieu au sein de la communauté d'utilisateurs d'origine et que la Recommandation inclut une référence explicite à la version spécifique correspondante maintenue par la communauté d'utilisateurs. Ainsi, au moment de l'adoption initiale de la Recommandation UIT-T X.1525, une vérification approfondie et une déclaration d'équivalence seront faites; et toute modification apportée par la communauté

d'utilisateurs sera reportée en temps utile dans les versions ultérieures de la Recommandation dans le cadre d'une collaboration suivie.

La Recommandation UIT-T X.1525 – Système commun de notation des failles – a été élaborée en collaboration avec la société MITRE sans perdre de vue qu'il était important de maintenir, dans la mesure du possible, la compatibilité sur le plan technique avec le document "Common Weakness Scoring System (CWSS)", version 1.0.1, daté du 5 septembre 2014 [https://cwe.mitre.org/cwss/cwss_v1.0.1.html].

Recommandation UIT-T X.1525

Système commun de notation des failles

1 Domaine d'application

La présente Recommandation propose une approche normalisée pour la communication des caractéristiques et des incidences des failles au moment de la conception des fonctionnalités des logiciels TIC, utilisant des métriques environnementales et de surface d'attaque pour appliquer des informations contextuelles. Le système CWSS reflète de manière plus précise le risque pour l'utilisateur des logiciels, compte tenu du contexte d'activité particulier dans lequel ils fonctionneront pour l'utilisateur et des fonctionnalités particulières qu'ils assurent pour l'utilisateur.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 accès [b-UIT-T X.1521]: aptitude d'un sujet à voir, modifier ou communiquer avec un objet. L'accès donne lieu à un flux d'informations entre le sujet et l'objet.

3.1.2 disponibilité [b-UIT-T X.1521]: accès fiable et en temps utile par des personnes autorisées à des données et des ressources.

3.1.3 instance d'attaque [b-UIT-T X.1544]: attaque précise contre une application ou un système donné, qui cible les vulnérabilités ou les failles de ce système.

3.1.4 confidentialité [b-UIT-T X.1521]: principe de sécurité visant à faire en sorte que les informations ne soient pas divulguées à des sujets non autorisés.

3.1.5 intégrité [b-UIT-T X.1521]: principe de sécurité visant à faire en sorte que les informations et les systèmes ne soient pas modifiés de façon malveillante ou accidentelle.

3.1.6 risque [b-UIT-T X.1521]: impact relatif qu'aurait l'exploitation d'une vulnérabilité sur l'environnement d'un utilisateur.

3.1.7 menace [b-UIT-T X.1521]: probabilité ou fréquence d'apparition d'un événement préjudiciable.

3.1.8 vulnérabilité [b-UIT-T X.1500]: toute faille qui pourrait être exploitée pour violer un système ou les informations qu'il contient.

3.1.9 faille [b-UIT-T X.1524]: lacune ou imperfection dans le code, la conception, l'architecture ou le déploiement d'un logiciel qui pourrait, à un moment donné, devenir une vulnérabilité, ou pourrait contribuer à l'introduction d'autres vulnérabilités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

vignette: une vignette permet de définir de manière partageable et formalisée un environnement particulier, le rôle que les logiciels jouent dans cet environnement, et les priorités d'une organisation en ce qui concerne la sécurité des logiciels.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AI instance d'authentification (authentication instance)

AL couche des privilèges acquis (*acquired privilege layer*)

AP privilèges acquis (*acquired privilege*)

AS puissance d'authentification (*authentication strength*)

ASLR randomisation de la configuration de l'espace d'adresses (*address space layout randomization*)

AV vecteur d'accès (*access vector*)

BI impact sur les activités (*business impact*)

BVC contexte de valeur des activités (*business value context*)

CD disque compact (*compact disc*)

CIO directeur informatique (*chief information officer*)

CSO directeur de la sécurité (*chief security officer*)

CSRF falsification de requête intersites (*cross-site-request-forgery*)

CVSS système commun de notation des vulnérabilités (*common vulnerability scoring system*)

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

CWRAF cadre d'analyse des risques pour les failles courantes (*common weakness risk analysis framework*)

CWSS système commun de notation des failles (*common weakness scoring system*)

DI probabilité de découverte (*likelihood of discovery*)

DNS système des noms de domaine (*domain name system*)

DS domaine de déploiement (*deployment scope*)

EC efficacité du contrôle externe (*external control effectiveness*)

EX probabilité d'exploit (*likelihood of exploit*)

FC confiance dans le résultat (*finding confidence*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

HTML langage de balisage hypertexte (*hyper text markup language*)

IC efficacité du contrôle interne (*efficacité du contrôle interne*)

TIC	technologies de l'information et de la communication
IN	niveau d'interaction (*level of interaction*)
IP	protocole Internet (*internet protocol*)
NIST	National Institute of Standards and Technology
OS	système d'exploitation (*operating system*)
OWASP	projet ouvert concernant la sécurité des applications web (*open web application security project*)
P	prévalence (*prevalence*)
PCI DSS	norme sur la sécurité des données pour les cartes de paiement (*payment card industry data security standard*)
RL	couche des privilèges requis (*required privilege layer*)
RP	privilèges requis (*required privilege*)
SAMATE	évaluation des métriques et des outils concernant l'assurance logicielle (*software assurance metrics and tool evaluation*)
SANS	administration des systèmes, audit, réseaux et sécurité (*sysadmin, audit, networking, and security*)
SQL	langage de requête structuré (*structured query language*)
SSL	couche de connecteurs sécurisés (*secure sockets layer*)
TI	impact technique (*technical impact*)
TLS	sécurité de la couche transport (*transport layer security*)
USB	bus série universel (*universal serial bus*)
XSS	exécution de script intersites (*cross site scripting*)

5 Conventions

Aucune.

6 Utilisation du CWSS

A l'heure actuelle, les concepteurs de logiciels, gestionnaires, testeurs, fournisseurs de systèmes de sécurité et prestataires de services, acheteurs, fournisseurs d'applications et chercheurs dans le domaine des TIC doivent identifier et évaluer les failles dans les logiciels qui pourraient se traduire par des vulnérabilités au moment de l'utilisation des logiciels. Ils doivent ensuite pouvoir prioriser ces failles et déterminer celles qui présentent les plus grands risques afin d'y remédier. Lorsqu'il faut remédier à un grand nombre de failles, chacune étant notée sur des échelles différentes, les divers membres de la communauté des TIC, gestionnaires, testeurs, acheteurs et concepteurs, s'en remettent à leurs propres méthodologies pour trouver des moyens de comparer des failles disparates et de les traduire en informations décisionnelles. Le système commun de notation des failles (CWSS) est un cadre ouvert qui traite de cette question. Il offre les avantages suivants:

- Mesures quantitatives: le CWSS fournit une mesure quantitative des failles non résolues qui pourraient être présentes dans une application logicielle.
- Cadre commun: le CWSS offre un cadre commun permettant de prioriser les erreurs de sécurité ("failles") qui sont découvertes dans les applications logicielles.
- Priorisation personnalisée: conjointement avec le Common Weakness Risk Analysis Framework (CWRAF) [b-CWRAF], le CWSS peut être utilisé par les consommateurs pour

identifier les types de failles les plus importants pour leurs domaines d'activité, afin de servir de base à leurs activités d'acquisition et de protection dans le cadre du processus plus large d'obtention de l'assurance logicielle.

6.1 Description du CWSS

Le CWSS est organisé en trois *groupes de métriques*: résultat de base, surface d'attaque, et environnement, comme indiqué sur la Figure 1. Chaque groupe contient plusieurs métriques – également appelées *facteurs* – qui sont utilisées pour calculer une note CWSS pour une faille.

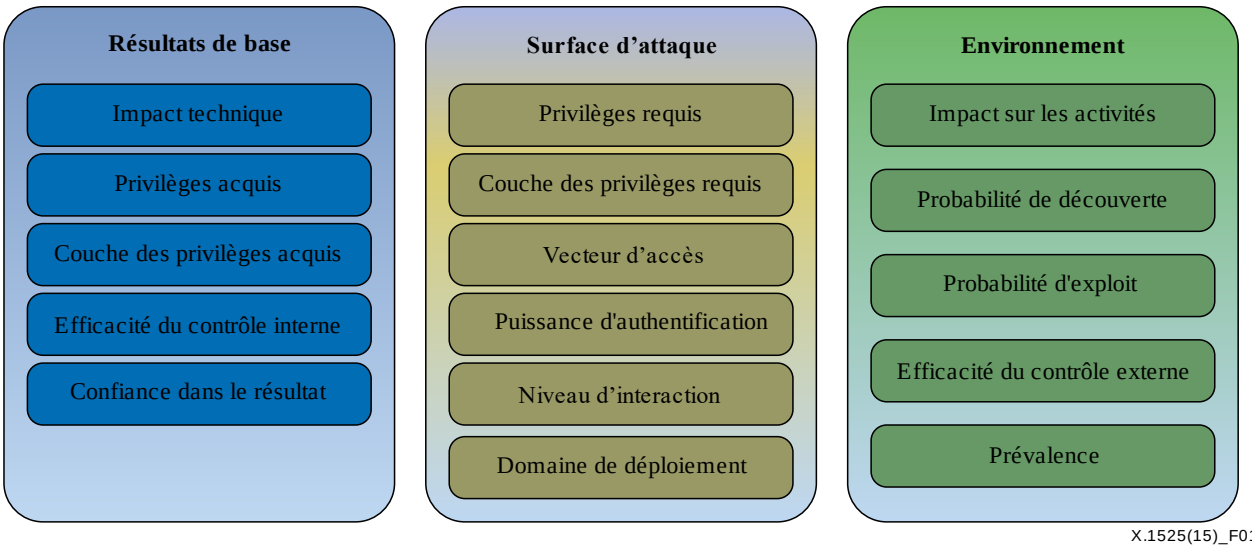

Figure 1 – Groupes de métriques du CWSS

Ces groupes de métriques sont décrits comme suit:

- Groupe de métriques du résultat de base: représente le risque intrinsèque posé par la faille, la confiance dans la précision du résultat, et la puissance des contrôles. Ce groupe de métriques est examiné au § 7.3.
- Groupe de métriques de la surface d'attaque: représente les obstacles qu'un attaquant doit surmonter pour pouvoir exploiter la faille. Ce groupe de métriques est examiné au § 7.4.
- Groupe de métriques de l'environnement: représente les caractéristiques de la faille qui sont propres à un environnement ou à un contexte opérationnel particulier. Ce groupe de métriques est examiné au § 7.5.

6.2 Fonctionnement du CWSS

Une valeur est attribuée à chaque facteur du groupe des métriques du résultat de base. Les valeurs obtenues sont converties en leur poids associé, et une sous-note résultat de base est calculée. Cette sous-note est comprise entre 0 et 100. La même méthode est appliquée aux groupes de métriques de la surface d'attaque et de l'environnement, les sous-notes obtenues étant comprises entre 0 et 1. Enfin, les trois sous-notes sont multipliées ensemble et on obtient une note CWSS comprise entre 0 et 100, comme illustré ci-après à la Figure 2.

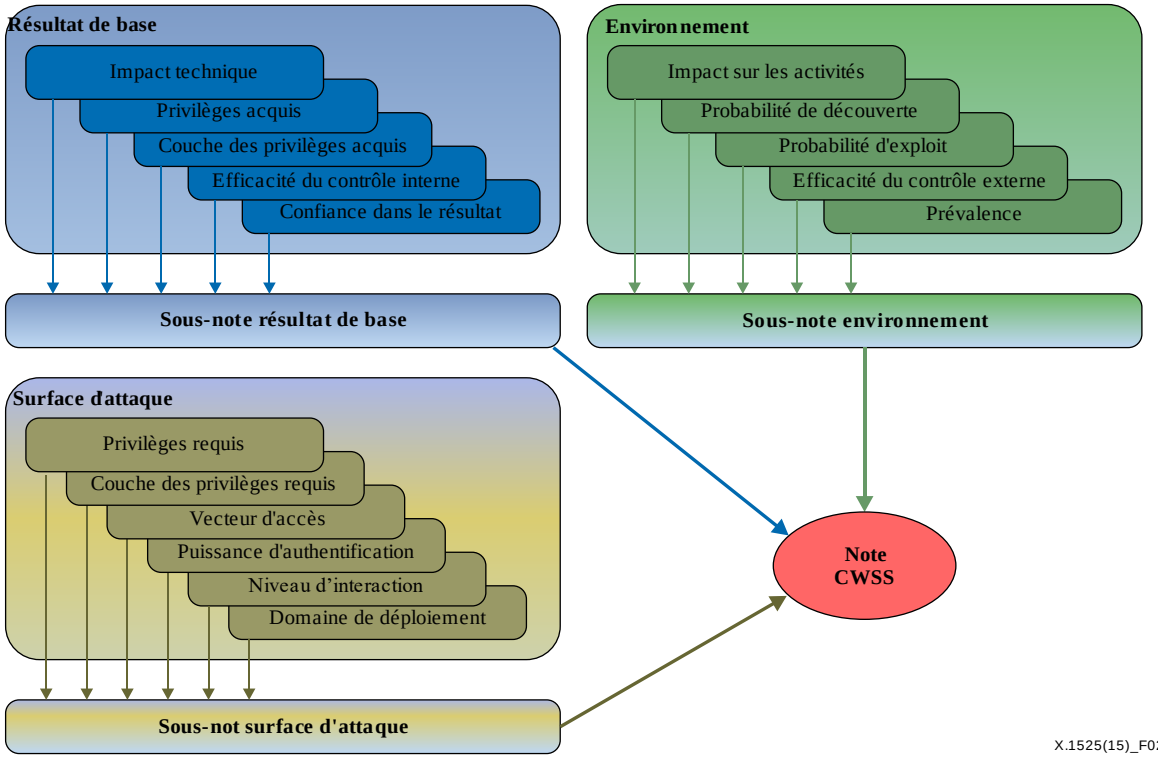

Figure 2 – Notation du CWSS

6.3 Notation du CWSS

La communauté des parties prenantes travaille en collaboration avec MITRE à l'étude de plusieurs méthodes de notation différentes qui devront peut-être être prises en charge dans le cadre du CWSS. On compte actuellement les quatre méthodes de notation suivantes:

Ciblée — Cette méthode note chacune des failles découvertes dans la conception ou la mise en œuvre d'un progiciel donné ("méthode ciblée"), par exemple un débordement de tampon associé au nom d'utilisateur d'un programme d'authentification à la ligne 1234 du serveur.c dans un progiciel de serveur FTP. Les outils automatiques et les consultants en sécurité des logiciels utilisent des méthodes ciblées lorsqu'ils évaluent la sécurité d'un progiciel sur la base des failles qu'il contient.

Généralisée — Cette méthode note les catégories de failles indépendamment de tout logiciel particulier, afin de les prioriser (par exemple " la priorité est accordée aux débordements de tampon par rapport aux fuites de mémoire"). Cette approche est notamment utilisée par le CWE/SANS Top 25 et l'OWASP Top Ten, mais aussi par certains analyseurs de code automatiques. Il se pourrait que les notes généralisées soient très différentes des notes ciblées obtenues à partir d'une analyse complète de chacune des manifestations de la catégorie de failles dans un progiciel donné. Par exemple, la catégorie des débordements de tampon reste très importante pour de nombreux concepteurs, mais certains bogues liés à un débordement de tampon pourraient être considérés comme moins importants s'ils ne peuvent pas être exploités directement par un attaquant et si leur impact est réduit du fait de la présence de mécanismes de protection au niveau du système d'exploitation (OS) tels que la randomisation de la configuration de l'espace d'adresses (ASLR).

Adaptée au contexte — Cette méthode associe les notes en fonction des besoins d'un contexte analytique donné pouvant intégrer des priorités liées aux activités/à la mission, des environnements de menaces, une tolérance aux risques, etc. Ces besoins sont définis à l'aide de vignettes qui relient les caractéristiques intrinsèques des failles aux considérations de niveau supérieur relatives aux activités de l'entreprise. Cette méthode pourrait être appliquée à la fois avec la notation ciblée et à la notation généralisée.

Agrégée — Cette méthode associe les résultats de plusieurs notes de faille de niveau inférieur pour produire une seule note générale. L'agrégation s'appliquerait avant tout à la notation ciblée, mais elle pourrait aussi être utilisée avec la notation généralisée, comme cela a été le cas pour le CWE/SANS Top 25 de 2010.

Il est à noter que l'essentiel des discussions au sujet du CWSS porte actuellement sur la méthode de notation ciblée et un cadre applicable à la notation adaptée au contexte. L'examen des méthodes de notation agrégée viendra après. La notation généralisée est étudiée séparément, principalement dans le cadre du Top 25 de 2011 et du CWRAF.

Les notes CWSS peuvent être calculées automatiquement, par exemple par un outil d'analyse du code, ou manuellement par un consultant en sécurité des logiciels ou par un concepteur de logiciels. Étant donné qu'il est peu probable que les outils d'analyse automatique aient accès à certaines informations telles que l'environnement d'exploitation de l'application, la notation CWSS pourrait éventuellement se faire en plusieurs étapes: un outil calcule d'abord automatiquement des notes CWSS, puis un analyste humain ajoute manuellement des détails supplémentaires et recalcule les notes.

6.4 Utilisateurs du CWSS

Pour une efficacité optimale, le CWSS prend en charge plusieurs scénarios d'utilisation par différentes parties prenantes qui sont toutes intéressées par un système de notation cohérent pour prioriser les failles dans les logiciels qui pourraient entraîner des risques au niveau des produits, systèmes, réseaux et services. Les principales parties prenantes sont notamment les suivantes:

- Concepteurs de logiciels: les concepteurs travaillent souvent avec des délais serrés, en raison des cycles de commercialisation et des ressources limitées. Ils ne sont donc pas en mesure d'étudier et de résoudre toutes les failles signalées. Ils peuvent choisir de se concentrer sur les problèmes les plus graves ou les plus faciles à résoudre. Dans le cas de résultats automatiques signalant des failles, ils pourraient choisir de se concentrer sur les résultats qui ont le moins de chances d'être des faux positifs.
- Responsables de la conception de logiciels: les responsables de la conception de logiciels créent des stratégies pour prioriser les catégories de failles et supprimer des catégories entières de failles dans toute la base du code, ou au moins la partie considérée comme étant la plus en danger, éventuellement en définissant des listes personnalisées des N premières failles. Ils doivent comprendre ce que l'intégration de logiciels de tierce partie, qui peuvent contenir leurs propres failles, peut avoir en termes de sécurité. Ils peuvent être amenés à définir des exigences de sécurité et des priorités distinctes pour chaque ligne de produits.
- Acquéreurs de logiciels: les clients, y compris le personnel chargé de l'acquisition, veulent obtenir des logiciels de tierce partie avec un niveau raisonnable d'assurance que le fournisseur de logiciels a dûment procédé à la suppression ou à la prévention des failles les plus critiques pour les activités et la mission de l'acquéreur. Les parties prenantes connexes comprennent les directeurs informatiques (CIO), les directeurs de la sécurité (CSO), les administrateurs système, et les utilisateurs finals des logiciels.
- Responsables de la sécurité de l'entreprise: les responsables de la sécurité de l'entreprise cherchent à réduire autant que possible le risque au sein de leur entreprise, à la fois en ce

qui concerne les vulnérabilités bien connues dans les produits de tierce partie, et les vulnérabilités (ou failles) dans leurs propres logiciels internes. Ils souhaiteront peut-être utiliser un mécanisme de notation qui puisse être intégré avec d'autres processus de gestion de la sécurité, par exemple pour combiner les résultats de l'analyse des vulnérabilités dans les produits de tierce partie (concernant les vulnérabilités connues dans les produits de tierce partie) avec une analyse de l'application personnalisée (concernant les logiciels internes) afin de faciliter l'évaluation du risque général pour un actif.

- Fournisseurs de systèmes d'analyse de code et consultants: les fournisseurs et consultants ont souvent leurs propres techniques de notation personnalisées, mais ils veulent fournir un mécanisme de notation approuvé par la communauté et cohérent pour différents clients.
- Évaluateurs des capacités d'analyse du code: les évaluateurs analysent et mesurent les capacités des techniques d'analyse du code (par exemple NIST SAMATE). Ils pourraient utiliser un mécanisme cohérent de notation des failles pour pouvoir analyser les résultats signalés, et comprendre le degré de gravité de ces résultats sans devoir recourir à des méthodes de notation au cas par cas qui peuvent dépendre dans une large mesure de l'outil ou de la technique.
- Autres parties prenantes: parmi les autres parties prenantes, pourront figurer des chercheurs dans le domaine des vulnérabilités, des défenseurs d'une conception sécurisée, et des analystes se fondant sur la conformité (par exemple PCI DSS).

En juin 2014 (version active: CWSS 0.8), on compte plusieurs mises en œuvre pratiques du CWSS, avec comme principaux utilisateurs des fournisseurs de systèmes d'analyse de code et des consultants en sécurité des logiciels.

7 Groupes de métriques

7.1 Facteurs des groupes de métriques

Le CWSS contient les facteurs ci-après, organisés par groupes de métriques comme indiqué dans le Tableau 1 ci-dessous. Chaque facteur est décrit de manière plus détaillée dans les paragraphes qui suivent.

Tableau 1 – Facteurs des groupes de métriques

Groupe	Nom	Description succincte
Résultat de base	Impact technique (TI)	Résultat que la faille est susceptible de produire, dans l'hypothèse où on parvient à atteindre et à exploiter la faille.
	Privilèges acquis (AP)	Type de privilèges qui sont obtenus par un attaquant qui parvient à exploiter la faille.
	Couche des privilèges acquis (AL)	Couche opérationnelle dans laquelle l'attaquant obtient des privilèges en parvenant à exploiter la faille.
	Efficacité du contrôle interne (IC)	Aptitude du contrôle à faire en sorte que la faille ne puisse pas être exploitée par un attaquant.
	Confiance dans le résultat (FC)	Confiance dans le fait que le problème signalé est une faille qui peut être utilisée par un attaquant.
Surface d'attaque	Privilèges requis (RP)	Type de privilèges qu'un attaquant doit déjà avoir pour pouvoir atteindre le code/la fonctionnalité qui contient la faille.
	Couche des privilèges requis (RL)	Couche opérationnelle dans laquelle l'attaquant doit avoir des privilèges pour pouvoir tenter d'attaquer la faille.
	Vecteur d'accès (AV)	Canal par lequel un attaquant doit communiquer pour atteindre le code ou la fonctionnalité qui contient la faille.
	Puissance d'authentification (AS)	Puissance du programme d'authentification qui protège le code/la fonctionnalité qui contient la faille.
	Niveau d'interaction (IN)	Actions requises de la part de la ou des victimes humaines pour qu'une attaque réussisse.
	Domaine de déploiement (SC)	Indique si la faille est présente dans toutes les instances de déploiement possible du logiciel, ou si elle est limitée à un sous-ensemble de plates-formes et/ou de configurations.
Environnement	Impact sur les activités (BI)	Impact potentiel sur les activités ou la mission de l'entreprise si on parvient à exploiter la faille.
	Probabilité de découverte (DI)	Probabilité qu'un attaquant puisse découvrir la faille.
	Probabilité d'exploit (EX)	Probabilité, si la faille est découverte, qu'un attaquant disposant des privilèges/de l'authentification/de l'accès requis parvienne à l'exploiter.
	Efficacité du contrôle externe (EC)	Aptitude des contrôles ou mesures d'atténuation externes au logiciel à faire en sorte qu'il soit plus difficile pour un attaquant d'atteindre et/ou d'exploiter la faille.
	Prévalence (P)	Fréquence d'apparition de ce type de faille dans les logiciels.

7.2 Valeurs pour l'incertitude et la souplesse

Le CWSS peut être utilisé dans les cas où on dispose de peu d'informations au départ, mais on disposera d'informations de meilleure qualité au fil du temps. Dans de nombreux cas d'utilisation, la note CWSS pour un résultat donné signalant une faille risquera de changer fréquemment, au fur et à mesure de la découverte de davantage d'informations. Des entités différentes pourront évaluer des facteurs distincts à différents moments.

En tant que tel, chaque facteur CWSS a de fait des caractéristiques "environnementales" ou "temporelles", de sorte qu'il n'est pas particulièrement utile d'adopter les mêmes types de groupes de métriques que ceux qui sont utilisés dans le CVSS.

La plupart des facteurs ont en commun les quatre valeurs indiquées dans le Tableau 2.

Tableau 2 – Valeurs des facteurs pour l'incertitude et la souplesse

Valeur	Utilisation
Inconnu	L'entité qui calcule la note n'a pas assez d'informations pour pouvoir attribuer une valeur au facteur. Ce peut être un signal appelant à poursuivre l'analyse. Par exemple, il se pourrait qu'un analyseur de code automatique puisse trouver certaines failles, mais ne puisse pas détecter la présence ou non de mécanismes d'authentification. L'utilisation de la valeur "inconnu" souligne le fait que la note est incomplète ou estimée, et qu'une analyse complémentaire peut être nécessaire. Ainsi, la modélisation des informations incomplètes est simplifiée, et le contexte de valeur des activités peut plus facilement influer sur les notes finales qui ont été générées au moyen d'informations incomplètes. Le poids pour cette valeur est de 0,5 pour tous les facteurs, ce qui a généralement pour effet de produire une note plus faible; l'ajout de nouvelles informations (à savoir le passage de certains facteurs de la valeur "inconnu" à une autre valeur) permettra ensuite d'ajuster la note vers le haut ou vers le bas sur la base des nouvelles informations.
Non applicable	Le facteur est explicitement ignoré dans le calcul de la note, ce qui permet, de fait, au contexte de valeur des activités a la possibilité d'imposer qu'un facteur soit pris en compte ou ignoré dans la note finale. Par exemple, une méthode de notation CWSS axée sur un client pourrait ignorer les mesures correctives, et un environnement à haut degré d'assurance pourrait nécessiter d'analyser tous les résultats signalés, même si le niveau de confiance dans leur précision est faible. Pour un ensemble de résultats signalant des failles dans un progiciel donné, tous les résultats devraient avoir la même valeur "non applicable" pour le facteur qui est ignoré.
Quantifié	Pour l'attribution d'un poids au facteur, on peut utiliser l'intervalle continu et quantifié allant de 0,0 à 1,0, plutôt que l'ensemble de valeurs discrètes définies pour le facteur. Les facteurs ne sont pas tous quantifiables de cette manière, mais cela permet une personnalisation supplémentaire de la métrique.
Valeur par défaut	Le poids du facteur peut être mis à une valeur par défaut. L'étiquetage du facteur comme ayant la valeur par défaut permet de procéder ultérieurement à une analyse et à une éventuelle modification.

7.3 Groupe des métriques du résultat de base

Le groupe des métriques du résultat de base est constitué des facteurs suivants:

- Impact technique (TI)
- Privilèges acquis (AP)
- Couche des privilèges acquis (AL)
- Efficacité du contrôle interne (IC)
- Confiance dans le résultat (FC)

La combinaison des valeurs de l'impact technique, des privilèges acquis, et de la couche des privilèges acquis donne à l'utilisateur une certaine puissance d'expression. Par exemple, l'utilisateur peut caractériser un impact technique "élevé" avec le privilège "administrateur" au niveau de la couche "application".

7.3.1 Impact technique (TI)

L'impact technique est le résultat que la faille est susceptible de produire, dans l'hypothèse où on parvient à atteindre et à exploiter la faille. Il est exprimé avec une granularité plus fine que la confidentialité, l'intégrité et la disponibilité.

L'impact technique devrait être évalué par rapport aux privilèges acquis (AP) et à la couche des privilèges acquis (AL).

Tableau 3 – Poids de l'impact technique

Valeur	Code	Poids	Description
Critique	C	1,0	Contrôle complet du logiciel analysé, à tel point que les opérations sont impossibles.
Élevé	H	0,9	Contrôle important du logiciel analysé, ou possibilité d'accéder à des informations critiques.
Moyen	M	0,6	Contrôle modéré du logiciel analysé, ou possibilité d'accéder à des informations modérément importantes.
Faible	L	0,3	Contrôle minime du logiciel analysé, ou possibilité d'accéder uniquement à des informations relativement peu importantes.
Aucun	N	0,0	Pas d'impact technique du tout sur le logiciel analysé. En d'autres termes, cette faille ne conduit pas à une vulnérabilité.
Valeur par défaut	D	0,6	Le poids pour la valeur par défaut est la valeur médiane des poids pour les valeurs critique, élevé, moyen, faible et aucun.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance; l'utilisateur pourrait vouloir analyser chaque résultat considéré signalant une faille, indépendamment de la confiance.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

Si cet ensemble de valeurs n'est pas assez précis, les utilisateurs du CWSS peuvent utiliser leurs propres méthodes quantifiées pour obtenir une sous-note. L'une de ces méthodes repose sur l'utilisation du Common Weakness Risk Analysis Framework (CWRAF) [b-CWRAF] pour définir une vignette et une fiche de notation de l'impact technique. Le poids de l'impact est calculé au moyen de valeurs d'importance propres à la vignette pour différents impacts techniques qui pourraient découler de l'exploitation de la faille, comme la modification de données sensibles, l'obtention de privilèges, la consommation de ressources, etc.

7.3.2 Privilèges acquis (AP)

Les privilèges acquis indiquent le type de privilèges qui sont obtenus par un attaquant qui parvient à exploiter la faille.

Il est à noter que les valeurs sont les mêmes que pour les privilèges requis, mais que les poids sont différents.

Dans certains cas, la valeur pour les privilèges acquis peut être la même que pour les privilèges requis, ce qui implique soit (1) l'escalade de privilèges au niveau "horizontal" (p.ex. d'un utilisateur dépourvu de privilège à un autre) soit (2) l'escalade de privilèges dans un sandbox, par exemple un utilisateur utilisant uniquement le protocole de transfert de fichiers (FTP) qui peut s'échapper vers l'interface système.

Tableau 4 – Poids des privilèges acquis

Valeur	Code (Note)	Poids	Description
Administrateur	A	1,0	L'attaquant parvient à accéder à une entité disposant de privilèges administrateur, racine, SYSTÈME, ou de privilèges équivalents qui lui donnent un contrôle total du logiciel analysé; ou l'attaquant parvient à passer de ses propres privilèges (de niveau inférieur) aux privilèges administrateur.
Utilisateur disposant de privilèges partiels	P	0,9	L'attaquant parvient à accéder à une entité disposant de certains privilèges particuliers, mais pas de tous les privilèges administrateur; ou l'attaquant parvient à passer de ses propres privilèges (de niveau inférieur) à ceux d'un utilisateur disposant de privilèges partiels. Par exemple, un utilisateur pourrait avoir des privilèges pour faire des sauvegardes, mais pas pour modifier la configuration de logiciels ou installer des mises à jour.
Utilisateur normal	RU	0,7	L'attaquant parvient à accéder à une entité qui est un utilisateur normal ne disposant pas de privilèges particuliers; ou l'attaquant parvient à passer de ses propres privilèges (de niveau inférieur) à ceux d'un utilisateur normal.
Privilèges limités/ invité	L	0,6	L'attaquant parvient à accéder à une entité disposant de privilèges limités ou "invité", qui peuvent restreindre considérablement les activités admissibles; ou l'attaquant parvient à passer de ses propres privilèges (de niveau inférieur) aux privilèges invité. Note: cette valeur n'a pas de rapport avec le concept de "système d'exploitation invité" dans les serveurs virtualisés.
Aucun	N	0,1	L'attaquant ne parvient pas à accéder à des privilèges supplémentaires par rapport à ceux dont il dispose déjà. (Il est à noter que cette valeur peut être utile dans des cas limités dans lesquels l'attaquant peut s'échapper d'un sandbox ou d'un autre environnement restrictif mais ne parvient pas malgré tout à obtenir des privilèges supplémentaires, ou à obtenir un accès comme les autres utilisateurs.)
Valeur par défaut	D	0,7	Valeur médiane des poids pour les valeurs aucun, invité, utilisateur normal, utilisateur disposant de privilèges partiels, et administrateur.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance et imposant une application stricte de la séparation des privilèges, y compris entre les utilisateurs disposant déjà de privilèges.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Il est à noter que la valeur quantifié est prise en charge dans un souci d'exhaustivité; toutefois, étant donné que les privilèges et les utilisateurs sont des entités discrètes, il se pourrait que les cas dans lesquels un modèle quantifié serait utile soient limités.
NOTE – Pour les principales valeurs de ce facteur, on peut utiliser l'acronyme "RUNLAP" (RU, N, L, A, P).			

7.3.3 Couche des privilèges acquis (AL)

La couche des privilèges acquis identifie la couche opérationnelle dans laquelle l'attaquant obtient des privilèges en parvenant à exploiter la faille.

Tableau 5 – Poids de la couche des privilèges acquis

Valeur	Code (Note)	Poids	Description
Application	A	1,0	L'attaquant acquiert les privilèges qui sont pris en charge dans le logiciel analysé proprement dit. (Si le logiciel analysé est une partie essentielle du système sous-jacent, par exemple le noyau d'un système d'exploitation, la valeur système sera peut-être plus appropriée.)
Système	S	0,9	L'attaquant acquiert les privilèges au niveau du système sous-jacent ou du serveur physique qui est utilisé pour exécuter le logiciel analysé.
Réseau	N	0,7	L'attaquant acquiert les privilèges permettant d'accéder au réseau.
Infrastructure de l'entreprise	E	1,0	L'attaquant acquiert les privilèges au niveau d'une pièce maîtresse de l'infrastructure de l'entreprise, par exemple un routeur, commutateur, système de noms de domaine (DNS), contrôleur de domaine, pare-feu, serveur d'identités, etc.
Valeur par défaut	D	0,9	Valeur médiane des poids pour les valeurs application, système, réseau et infrastructure de l'entreprise.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance et imposant une application stricte de la séparation des privilèges, y compris entre les utilisateurs disposant déjà de privilèges.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Il est à noter que la valeur quantifié est prise en charge dans un souci d'exhaustivité; toutefois, étant donné que les couches de privilège sont des entités discrètes, il se pourrait que les cas dans lesquels un modèle quantifié serait utile soient limités.
NOTE – Pour les valeurs principales de ce facteur, on peut utiliser l'acronyme "SANE" (S, A, N, E).			

7.3.4 Efficacité du contrôle interne (IC)

Un contrôle interne est un mécanisme de contrôle, de protection ou d'atténuation qui a été explicitement intégré dans le logiciel (dans le cadre de l'architecture, de la conception ou de la mise en œuvre). L'efficacité du contrôle interne mesure l'aptitude du contrôle à faire en sorte que la faille ne puisse pas être exploitée par un attaquant. Par exemple, un programme de validation des données d'entrée qui limite la longueur des données d'entrée à 15 caractères pourrait avoir une efficacité modérée vis-à-vis des attaques par exécution de scripts intersites (XSS) en réduisant la taille de l'exploit XSS qui peut être tenté.

Lorsqu'il existe plusieurs contrôles internes, ou plusieurs chemins de code permettant d'atteindre la même faille, les directives sont les suivantes:

- Pour chaque chemin de code, analyser chaque contrôle interne qui existe le long du chemin de code, et choisir la valeur correspondant au plus faible poids (c'est-à-dire le contrôle interne le plus puissant le long du chemin de code), appelée valeur de chemin de code.
- Collecter toutes les valeurs de chemin de code.

- Choisir la valeur de chemin de code qui correspond au poids le plus élevé (c'est-à-dire au contrôle le plus faible).

Cette méthode consiste à déterminer, pour chaque chemin de code, le contrôle le plus puissant (car un attaquant aurait à contourner ce contrôle), puis à choisir le chemin de code le plus faible (c'est-à-dire la route la plus facile que l'attaquant puisse prendre).

Tableau 6 – Poids de l'efficacité du contrôle interne

Valeur	Code	Poids	Description
Aucun	N	1,0	Il n'existe aucun contrôle.
Limité	L	0,9	Des méthodes simplistes ou des restrictions involontaires pourraient empêcher un attaquant ordinaire d'exploiter le problème.
Modéré	M	0,7	Le mécanisme de protection est couramment utilisé mais comporte des limitations connues qu'un attaquant connaisseur pourrait contourner moyennent certains efforts. Par exemple, le recours au codage d'entité HTML (langage de balisage hypertexte) pour empêcher les attaques XSS peut être contourné lorsque les données de sortie sont placées dans un autre contexte (attribut de feuilles de style en cascade ou de balise HTML par exemple).
Indirect (défense en profondeur)	I	0,5	Le contrôle n'assure pas de protection spécifique contre l'exploitation de la faille, mais il réduit indirectement l'impact lorsqu'une attaque parvient à être lancée, ou rend en tout cas plus difficile la construction d'un exploit fonctionnel. Par exemple, un programme de validation pourrait limiter indirectement la taille des données d'entrée, ce qui pourrait compliquer la tâche d'un attaquant qui souhaite construire des données pour une attaque XSS ou par injection SQL (langage de requête structuré).
Meilleur disponible	B	0,3	Le contrôle suit les meilleures pratiques existantes, mais il peut présenter certaines limitations qu'un attaquant expérimenté et déterminé peut surmonter, la présence d'autres failles étant éventuellement nécessaire. Par exemple, la méthode de la double soumission pour éviter la falsification de requête intersites (CSRF) est considérée comme offrant actuellement l'une des protections les plus puissantes, mais elle peut être contrecarrée en présence du comportement de certaines fonctionnalités qui peuvent lire les en-têtes HTTP bruts.
Complet	C	0,0	Le contrôle est parfaitement efficace contre la faille, autrement dit il n'y a ni bogue ni vulnérabilité, et aucune conséquence négative de l'exploitation du problème. Par exemple, une opération de copie de tampon garantissant que le tampon de destination est toujours plus volumineux que la source (plus toute augmentation indirecte de la taille de la source d'origine) n'entraînera pas de débordement.
Valeur par défaut	D	0,6	Valeur médiane des poids pour les valeurs complet, meilleur disponible, indirect, modéré, limité et aucun.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

7.3.5 Confiance dans le résultat (FC)

La confiance dans le résultat est la confiance dans le fait que le problème signalé:

1) est une faille; et
2) peut être exploité ou utilisé par un attaquant.

Tableau 7 – Poids de la confiance dans le résultat

Valeur	Code	Poids	Description
Véridique	T	1,0	La faille peut être atteinte par un attaquant.
Véridique localement	LT	0,8	La faille a lieu dans une fonction donnée ou un composant dont la conception repose sur l'invocation de cette fonction en toute sécurité, mais la possibilité pour un attaquant d'atteindre cette fonction est inconnue ou non présente. Par exemple, une fonction utilitaire pourrait élaborer une requête de base de données sans coder ses données d'entrée, mais si elle est appelée uniquement avec des chaînes constantes, le résultat est véridique localement.
Erroné	F	0,0	Le résultat est erroné (le résultat est un faux positif et il n'y a pas de faille), et/ou il n'y a pas de finalité possible pour l'attaquant.
Valeur par défaut	D	0,8	Valeur médiane des poids pour les valeurs véridique, véridique localement et erroné.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance; l'utilisateur pourrait vouloir analyser chaque résultat considéré signalant une faille, indépendamment de la confiance.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Certains outils d'analyse de code permettent de mesurer de manière précise la précision de diagrammes de détection spécifiques.

7.4 Groupe des métriques de la surface d'attaque

Le groupe de métriques de la surface d'attaque est constitué des facteurs suivants:

- Privilèges requis (RP)
- Couche des privilèges requis (RL)
- Vecteur d'accès (AV)
- Puissance d'authentification (AS)
- Niveau d'interaction (IN)
- Domaine de déploiement (SC).

7.4.1 Privilèges requis (RP)

Les privilèges requis indiquent le type de privilèges qu'un attaquant doit déjà avoir pour pouvoir atteindre le code/la fonctionnalité qui contient la faille.

Tableau 8 – Poids des privilèges requis

Valeur	Code (Note)	Poids	Description
Aucun	N	1,0	Aucun privilège n'est requis. Par exemple, il est possible qu'un moteur de recherche sur le web ne requière aucun privilège de la part d'une entité pour pouvoir lancer une recherche à partir d'un terme et visualiser les résultats.
Privilèges limités/ invité	L	0,9	L'entité dispose de privilèges limités ou "invité", qui peuvent restreindre considérablement les activités autorisées; l'entité pourrait être en mesure d'enregistrer ou de créer un nouveau compte sans exigence particulière ni preuve d'identité. Par exemple, un blog Internet pourrait permettre aux participants de créer un nom d'utilisateur et de soumettre une adresse électronique valable avant de saisir des commentaires. Note: cette valeur n'a pas de rapport avec le concept de "système d'exploitation invité" dans les serveurs virtualisés.
Utilisateur normal	RU	0,7	L'entité est un utilisateur normal qui ne dispose pas de privilèges particuliers.
Utilisateur disposant de privilèges partiels	P	0,6	L'entité est un utilisateur légitime disposant de certains privilèges particuliers, mais pas de tous les privilèges administrateur. Par exemple, un utilisateur pourrait avoir des privilèges pour faire des sauvegardes, mais pas pour modifier la configuration de logiciels ou installer des mises à jour.
Administrateur	A	0,1	L'entité dispose de privilèges administrateur, racine, SYSTÈME, ou de privilèges équivalents qui lui donnent un contrôle total du logiciel ou du système d'exploitation sous-jacent.
Valeur par défaut	D	0,7	Valeur médiane des poids pour les valeurs aucun, privilèges limités, utilisateur normal, utilisateur disposant de privilèges partiels et administrateur.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance et imposant une application stricte de la séparation des privilèges, y compris entre les utilisateurs disposant déjà de privilèges.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids normalisés. Il est à noter que la valeur quantifié est prise en charge dans un souci d'exhaustivité; toutefois, étant donné que les privilèges et les utilisateurs sont des entités discrètes, il se pourrait que les cas dans lesquels un modèle quantifié serait utile soient limités.
NOTE – Pour les valeurs principales de ce facteur, on peut utiliser l'acronyme "RUNLAP" (RU, N, L, A, P).			

7.4.2 Couche des privilèges requis (RL)

La couche des privilèges requis identifie la couche opérationnelle dans laquelle l'attaquant doit avoir des privilèges pour pouvoir tenter d'attaquer la faille.

Tableau 9 – Poids de la couche des privilèges requis

Valeur	Code (Note)	Poids	Description
Application	A	1,0	L'attaquant doit avoir les privilèges qui sont pris en charge dans le logiciel analysé proprement dit. (Si le logiciel analysé est une partie essentielle du système sous-jacent, par exemple le noyau d'un système d'exploitation, la valeur système sera peut-être plus appropriée.)
Système	S	0,9	L'attaquant doit avoir les privilèges au niveau du système sous-jacent ou du serveur physique qui est utilisé pour exécuter le logiciel analysé.
Réseau	N	0,7	L'attaquant doit avoir les privilèges permettant d'accéder au réseau.
Infrastructure de l'entreprise	E	1,0	L'attaquant doit avoir les privilèges au niveau d'une pièce maîtresse de l'infrastructure de l'entreprise, par exemple un routeur, commutateur, système de noms de domaine (DNS), contrôleur de domaine, pare-feu, serveur d'identités, etc.
Valeur par défaut	D	0,9	Valeur médiane des poids pour les valeurs application, système, réseau et infrastructure de l'entreprise.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance et imposant une application stricte de la séparation des privilèges, y compris entre les utilisateurs disposant déjà de privilèges.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Il est à noter que la valeur quantifié est prise en charge dans un souci d'exhaustivité; toutefois, étant donné que les couches de privilèges sont des entités discrètes, il se pourrait que les cas dans lesquels un modèle quantifié serait utile soient limités.
NOTE – Pour les valeurs principales de ce facteur, on peut utiliser l'acronyme "SANE" (S, A, N, E).			

7.4.3 Vecteur d'accès (AV)

Le vecteur d'accès identifie le canal par lequel un attaquant doit communiquer pour atteindre le code ou la fonctionnalité qui contient la faille. Il est à noter que ces valeurs sont très proches de celles utilisées dans le CVSS, à ceci près que le CWSS fait la distinction entre accès physique et accès local (interface système/compte).

Bien que le vecteur d'accès et la couche des privilèges requis soient étroitement liés, les deux sont distincts. Par exemple, un attaquant disposant d'un accès "physique" à un routeur pourrait toucher la couche réseau ou entreprise.

Tableau 10 – Poids du vecteur d'accès

Valeur	Code	Poids	Description
Internet	I	1,0	Un attaquant doit avoir accès à l'Internet pour pouvoir atteindre la faille.
Intranet	R	0,8	Un attaquant doit avoir accès à l'intranet d'une entreprise qui est protégé contre l'accès direct depuis l'Internet, par exemple au moyen d'un pare-feu, mais qui est accessible à la plupart des membres de l'entreprise.
Réseau privé	V	0,8	Un attaquant doit avoir accès à un réseau privé qui n'est accessible qu'à un ensemble défini et restreint de parties de confiance.
Réseau adjacent	A	0,7	Un attaquant doit avoir accès à une interface physique avec le réseau, par exemple au domaine de radiodiffusion ou de collision du logiciel vulnérable. Un sous-réseau IP local, un réseau Bluetooth, un réseau IEEE 802.11, et un segment Ethernet local sont des exemples de réseaux locaux.
Local	L	0,5	L'attaquant doit avoir un compte local interactif (interface système) en interaction directe avec le système d'exploitation sous-jacent.
Physique	P	0,2	L'attaquant doit avoir un accès physique au système sur lequel le logiciel est exécuté, ou bien doit être en mesure d'interagir avec le système via des interfaces telles qu'un bus série universel (USB), un disque compact (CD), un clavier, une souris, etc.
Valeur par défaut	D	0,75	Valeur médiane des poids pour les valeurs pertinentes.
Inconnu	U	0,5	
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Il est à noter que la valeur quantifié est prise en charge dans un souci d'exhaustivité; toutefois, étant donné que les vecteurs d'accès sont des entités discrètes, il se pourrait que les cas dans lesquels un modèle quantifié serait utile soient limités.

7.4.4 Puissance d'authentification (AS)

La puissance d'authentification correspond à la puissance du programme d'authentification qui protège le code/la fonctionnalité qui contient la faille.

Lorsque plusieurs programmes d'authentification sont utilisés, ou s'il existe deux chemins de code ou plus, il convient de procéder comme suit pour la notation:

Lorsqu'il existe plusieurs programmes d'authentification, ou plusieurs chemins de code permettant d'atteindre la même faille, les directives sont les suivantes:

- Pour chaque chemin de code, analyser chaque programme d'authentification qui existe le long du chemin de code, et choisir la valeur correspondant au plus faible poids (c'est-à-dire le programme d'authentification le plus puissant le long du chemin de code), appelée valeur de chemin de code.
- Collecter toutes les valeurs de chemin de code.
- Choisir la valeur de chemin de code qui correspond au poids le plus élevé (c'est-à-dire au programme le plus faible).

Cette méthode consiste à déterminer, pour chaque chemin de code, le programme d'authentification le plus puissant (car un attaquant aurait à contourner ce programme), puis à choisir le chemin de code le plus faible (c'est-à-dire la route la plus facile que l'attaquant puisse prendre).

Tableau 11 – Poids de la puissance d'authentification

Valeur	Code	Poids	Description
Puissant	S	0,7	La faille nécessite les méthodes les plus puissantes qui existent pour relier l'entité à une identité réelle, par exemple des jetons matériels et/ou une authentification à plusieurs facteurs.
Modéré	M	0,8	La faille nécessite une authentification au moyen de méthodes modérément puissantes, comme l'utilisation de certificats provenant d'autorités non fiables, une authentification basée sur la connaissance, ou des mots de passe à usage unique.
Faible	W	0,9	La faille nécessite une simple méthode d'authentification faible qu'il est facile de compromettre au moyen d'attaques par usurpation d'identité, dictionnaire, ou répétition (mot de passe statique par exemple).
Aucun	N	1,0	La faille ne nécessite aucune authentification du tout.
Valeur par défaut	D	0,85	Valeur médiane des poids pour les valeurs puissant, modéré, faible et aucun.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans un environnement exigeant un haut degré d'assurance et visant à éliminer toutes les failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

7.4.5 Niveau d'interaction (IN)

Le niveau d'interaction correspond aux actions requises de la part de la ou des victimes humaines pour qu'une attaque réussisse.

Tableau 12 – Poids du niveau d'interaction

Valeur	Code	Poids	Description
Automatique	A	1,0	Aucune interaction humaine n'est nécessaire.
Type/limité	T	0,9	L'attaquant doit convaincre l'utilisateur d'effectuer une action qui est courante ou considérée comme "normale" dans le cadre du fonctionnement type du produit. Par exemple, le fait de cliquer sur un lien dans une page web, ou de prévisualiser le contenu d'un courrier électronique, est un comportement courant.
Modéré	M	0,8	L'attaquant doit convaincre l'utilisateur d'effectuer une action qui pourrait sembler suspecte à un utilisateur prudent et connaisseur. Par exemple: l'utilisateur doit accepter un avertissement, laissant supposer que les données de l'attaquant pourraient avoir un contenu dangereux.
Opportuniste	O	0,3	L'attaquant ne peut pas avoir d'influence directe sur la victime, et peut uniquement tirer parti passivement d'erreurs ou d'actions commises par d'autres.
Elevé	H	0,1	Une ingénierie sociale de grande ampleur est requise, et éventuellement l'ignorance ou la négligence de la part de la victime.

Tableau 12 – Poids du niveau d'interaction

Valeur	Code	Poids	Description
Aucune interaction	NI	0,0	Aucune interaction n'est possible, pas même de manière opportuniste; ainsi la faille serait un "bogue" mais ne conduirait pas à une vulnérabilité. Etant donné que le CWSS concerne la sécurité, le poids est de 0.
Valeur par défaut	D	0,55	Valeur médiane des poids pour les valeurs automatique, limité, modéré, opportuniste, élevé et aucune interaction.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.

7.4.6 Domaine de déploiement (SC)

Le domaine de déploiement indique si la faille est présente dans toutes les instances de déploiement possible du logiciel, ou si elle est limitée à un sous-ensemble de plates-formes et/ou de configurations. Par exemple, il se pourrait qu'une erreur de calcul numérique concerne uniquement le logiciel exécuté dans le cadre d'un système d'exploitation particulier et d'une architecture à 64 bits, ou qu'un problème de traversée de chemin affecte uniquement les systèmes d'exploitation pour lesquels "\" est traité comme un séparateur de répertoires.

Tableau 13 – Poids du domaine de déploiement

Valeur	Code (Note 1)	Poids	Description
Tous	A	1,0	La faille est présente dans toutes les plates-formes ou configurations.
Modéré	M	0,9	La faille est présente dans les plates-formes ou configurations courantes.
Rare	R	0,5	La faille n'est présente que dans de rares plates-formes ou configurations.
Potentiellement atteignable	P	0,1	La faille est potentiellement atteignable (Note 2), mais tous les chemins de code sont actuellement sûrs, et/ou la faille se trouve dans du code mort,
Valeur par défaut	D	0,7	Valeur médiane des poids pour les valeurs RAMP
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. L'utilisateur pourra savoir quel pourcentage de logiciels mis sur le marché (ou pris en charge) contiennent ce bogue.
NOTE 1 − Pour les valeurs principales de ce facteur, on peut utiliser l'acronyme "RAMP" (R, A, M, P). NOTE 2 − Il existe un certain chevauchement entre la valeur "potentiellement atteignable" et la valeur "véridique localement" pour le facteur de confiance dans le résultat (FC).			

7.5 Groupe des métriques de l'environnement

Le groupe des métriques de l'environnement est constitué des facteurs suivants:

- Impact sur les activités (BI)
- Probabilité de découverte (DI)
- Probabilité d'exploit (EX)
- Efficacité du contrôle externe (EC)
- Prévalence (P).

7.5.1 Impact sur les activités (BI)

L'impact sur les activités décrit l'impact potentiel sur les activités ou la mission de l'entreprise si on parvient à exploiter la faille.

NOTE − Étant donné que les préoccupations au niveau de l'entreprise sont très variables d'une organisation à l'autre, le CWSS 1.0 ne cherche pas à entrer davantage dans les détails, par exemple en termes d'effets dommageables sur les plans financier, de la réputation, physique, juridique, etc. Ce facteur peut être quantifié afin de prendre en charge d'éventuels modèles définis à l'extérieur.

Tableau 14 – Poids de l'impact sur les activités

Valeur	Code	Poids	Description
Critique	C	1,0	Un échec des activités/de la mission pourrait avoir lieu.
Elevé	H	0,9	Les opérations relevant des activités/de la mission seraient considérablement impactées.
Moyen	M	0,6	Les activités/la mission seraient impactées, mais sans effets dommageables de grande ampleur sur les opérations normales.
Faible	L	0,3	Impact minime sur les activités/la mission.
Aucun	N	0,0	Aucun impact.
Valeur par défaut	D	0,6	Valeur médiane des poids pour les valeurs critique, élevé, moyen, faible et aucun.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer dans les contextes dans lesquels l'impact sur les activités n'entre pas en ligne de compte, ou si l'impact est évalué et considéré dans des processus analytiques qui n'entrent pas dans le cadre de la note CWSS proprement dite.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Il se pourrait par exemple que certaines organisations aient des mesures spécifiques pour évaluer la valeur des actifs pour les activités, mesures qui pourraient être intégrées dans la mesure de ce facteur.

7.5.2 Probabilité de découverte (DI)

La probabilité de découverte est la probabilité qu'un attaquant puisse découvrir la faille.

NOTE − Il a été envisagé de supprimer ce facteur dans le CWSS 1.0, car c'est un facteur qui peut être difficile à mesurer et qui peut dépendre d'autres facteurs tels que les privilèges acquis, l'impact technique et la prévalence. Toutefois, ce facteur a été conservé pour tenir compte du fait que certains concepteurs

utiliseront la probabilité de découverte pour les aider à déterminer avec quelle rapidité un problème devrait être résolu.

Tableau 15 – Poids de la probabilité de découverte

Valeur	Code	Poids	Description
Élevé	H	1,0	Il est très probable qu'un attaquant puisse découvrir la faille rapidement et moyennant peu d'efforts en utilisant des techniques simples, sans accéder au code source ou à d'autres artefacts qui simplifient la détection des failles.
Moyen	M	0,6	Il se pourrait qu'un attaquant soit en mesure de découvrir la faille, mais pour ce faire, certaines compétences seraient nécessaires, avec éventuellement la nécessité d'accéder au code source ou d'avoir des connaissances en ingénierie inverse. Pour pouvoir découvrir le problème, il faudra peut-être y consacrer un certain temps.
Faible	L	0,2	Il est peu probable qu'un attaquant découvre la faille s'il ne possède pas des compétences hautement spécialisées, s'il n'a pas accès au code source (ou à un équivalent), et s'il n'y consacre pas beaucoup de temps.
Valeur par défaut	D	0,6	Valeur médiane des poids pour les valeurs élevé, moyen et faible.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Ce facteur pourrait ne pas s'appliquer lorsque le calculateur de la note suppose que toutes les failles seront découvertes par un attaquant.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

7.5.3 Probabilité d'exploit (EX)

La probabilité d'exploit est la probabilité, si la faille est découverte, qu'un attaquant disposant des privilèges/de l'authentification/de l'accès requis parvienne à l'exploiter.

Tableau 16 – Poids de la probabilité d'exploit

Valeur	Code	Poids	Description
Élevé	H	1,0	Il est très probable qu'un attaquant parvienne à cibler cette faille, avec un exploit fiable qui est facile à développer.
Moyen	M	0,6	Il est probable qu'un attaquant parvienne à cibler cette faille, mais les chances de réussite pourraient varier, ou plusieurs tentatives pourraient être nécessaires avant de réussir.
Faible	L	0,2	Un attaquant ne ciblerait probablement pas cette faille, ou aurait très peu de chances de réussite.
Aucun	N	0,0	Un attaquant n'a aucune chance de réussite; autrement dit le problème est un "bogue" car il n'y a ni finalité ni avantage pour l'attaquant.
Valeur par défaut	D	0,6	Valeur médiane des poids pour les valeurs élevé, moyen et faible. La valeur "aucun" est ignorée, l'idée étant que peu de résultats relatifs signalant des failles seraient notés avec cette valeur, et que l'inclusion de cette valeur dans

Tableau 16 – Poids de la probabilité d'exploit

Valeur	Code	Poids	Description
			le calcul de la valeur médiane ramènerait le poids à un niveau non intuitif.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Par exemple, il se pourrait que le calculateur de la note veuille supposer que les attaquants pourront exploiter n'importe quelle faille qu'ils trouveront, ou seront enclins à investir d'importantes ressources pour contourner tous les éventuels obstacles pour parvenir à leurs fins.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

Il est à noter que ce facteur dépend de l'impact d'une faille, étant donné que les attaquants ciblent souvent les failles qui ont les impacts les plus graves. Il se peut aussi que les attaquants ciblent les failles qui sont faciles à exploiter. Ce facteur dépend aussi d'autres facteurs tels que l'efficacité du contrôle interne et du contrôle externe.

Il se pourrait que la prévalence ait aussi une incidence, mais la prévalence est plus étroitement liée à la probabilité de découverte.

7.5.4 Efficacité du contrôle externe (EC)

L'efficacité du contrôle externe est l'aptitude des contrôles ou mesures d'atténuation externes au logiciel à faire en sorte qu'il soit plus difficile pour un attaquant d'atteindre et/ou d'exploiter la faille. Par exemple, la randomisation de la configuration de l'espace d'adresses (ASLR) et des technologies analogues réduisent, mais n'éliminent pas, les chances de réussite d'une attaque par débordement de tampon. Toutefois, l'ASLR n'est pas directement instanciée dans le logiciel proprement dit.

Lorsqu'il existe plusieurs contrôles externes, ou plusieurs chemins de code permettant d'atteindre la même faille, les directives sont les suivantes:

- Pour chaque chemin de code, analyser chaque contrôle externe qui existe le long du chemin de code, et choisir la valeur correspondant au plus faible poids (c'est-à-dire le contrôle externe le plus puissant le long du chemin de code), appelée valeur de chemin de code.
- Collecter toutes les valeurs de chemin de code.
- Choisir la valeur de chemin de code qui correspond au poids le plus élevé (c'est-à-dire au contrôle le plus faible).

Cette méthode consiste à déterminer, pour chaque chemin de code, le contrôle le plus puissant (car un attaquant aurait à contourner ce contrôle), puis à choisir le chemin de code le plus faible (c'est-à-dire la route la plus facile que l'attaquant puisse prendre).

Tableau 17 – Poids de l'efficacité du contrôle externe

Valeur	Code	Poids	Description
Aucun	N	1,0	Il n'existe aucun contrôle.
Limité	L	0,9	Des méthodes simplistes ou des restrictions involontaires pourraient empêcher un attaquant ordinaire d'exploiter le problème.
Modéré	M	0,7	Le mécanisme de protection est couramment utilisé mais comporte des limitations connues qu'un attaquant connaisseur pourrait contourner moyennent certains efforts.
Indirect (défense en profondeur)	I	0,5	Le contrôle n'assure pas de protection spécifique contre l'exploitation de la faille, mais il réduit indirectement l'impact lorsqu'une attaque parvient à être lancée, ou rend en tout cas plus difficile la construction d'un exploit fonctionnel. Par exemple, la randomisation de la configuration de l'espace d'adresses (ASLR) et des technologies analogues réduisent, mais n'éliminent pas, les chances de réussite d'une attaque par débordement de tampon. Etant donné que la réponse consiste généralement à sortir du processus, le résultat est toujours un déni de service.
Meilleur disponible	B	0,3	Le contrôle suit les meilleures pratiques existantes, mais il peut présenter certaines limitations qu'un attaquant expérimenté et déterminé peut surmonter, la présence d'autres failles étant éventuellement nécessaire. Par exemple, la sécurité de la couche transport (TLS) / la couche de connecteurs sécurisés (SSL 3) sont opérationnelles dans une grande partie du web, et les méthodes plus puissantes ne sont généralement pas disponibles en raison de problèmes de compatibilité.
Complet	C	0,1	Le contrôle est parfaitement efficace contre la faille, autrement dit il n'y a ni bogue ni vulnérabilité, et aucune conséquence négative de l'exploitation du problème. Par exemple, un environnement sandbox pourrait restreindre à un seul répertoire de travail les opérations d'accès aux fichiers, ce qui permettrait d'assurer une protection contre l'exploitation de la traversée de chemins. Un poids non nul est utilisé afin de tenir compte de la possibilité que le contrôle externe puisse être supprimé involontairement dans l'avenir, par exemple en cas de modification de l'environnement du logiciel.
Valeur par défaut	D	0,6	Valeur médiane des poids pour les valeurs complet, meilleur disponible, indirect, modéré, limité et aucun.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés.

7.5.5 Prévalence (P)

La prévalence d'un résultat indique la fréquence d'apparition de ce type de faille dans les logiciels.

NOTE − Il pourrait être envisagé de supprimer ce facteur dans de futures versions. Toutefois, il est trop étroitement lié aux méthodes de notation généralisée et au CWRAF pour être supprimé dans le CWSS 1.0.

Ce facteur est destiné à être utilisé pour la notation généralisée de catégories de failles, par exemple pour l'élaboration de listes personnalisées des N premières failles. Lors de la notation d'un résultat

individuel signalant une faille dans un contexte de balayage automatique, on utilisera probablement la valeur "non applicable" pour ce facteur.

Tableau 18 – Poids de la prévalence

Valeur	Code	Poids (Note)	Description
Répandu	W	1,0	La faille se trouve dans la plupart voire la totalité des logiciels dans l'environnement associé, et plusieurs occurrences sont possibles dans le même progiciel.
Élevé	H	0,9	La faille est rencontrée très souvent, mais elle n'est pas répandue.
Courant	C	0,8	La faille est rencontrée périodiquement.
Limité	L	0,7	La faille est rencontrée rarement, voire jamais.
Valeur par défaut	D	0,85	Valeur médiane des poids pour les valeurs limité, courant, élevé et répandu.
Inconnu	UK	0,5	Les informations sont insuffisantes pour fournir une valeur pour ce facteur. Une analyse complémentaire pourra être nécessaire. Dans l'avenir, une valeur différente pourra être choisie, qui pourrait avoir une incidence sur la note.
Non applicable	NA	1,0	Ce facteur est intentionnellement ignoré dans le calcul de la note car il n'entre pas en ligne de compte dans la manière dont le calculateur de la note priorise les failles. Lors de la notation ciblée d'un résultat donné signalant une faille dans une application, la prévalence ne devrait pas en principe entrer en ligne de compte, car l'application considérée et les techniques analytiques déterminent la fréquence d'apparition de la faille, et de nombreuses méthodes de notation agrégée produiront des notes plus élevées s'il y a davantage de failles.
Quantifié	Q		Ce facteur pourrait être quantifié au moyen de poids personnalisés. Des données de prévalence précises peuvent être disponibles dans des cas d'utilisation limités, sous réserve que l'utilisateur recherche des données sur les failles à un bas niveau de granularité. Par exemple, un concepteur peut rechercher les failles dans une suite de produits, ou un fournisseur de systèmes d'audit de code pourrait mesurer la prévalence à partir des logiciels analysés parmi toute sa clientèle. Dans une version précédente du CWSS, la prévalence était calculée à partir des données de vote brutes collectées pour les 25 premières failles en 2010, qui utilisaient des valeurs discrètes (intervalle de 1 à 4) projetées ensuite sur un intervalle de 1 à 10.
NOTE − Étant donné que l'attaque d'un logiciel peut réussir même en présence d'une seule faille, les poids choisis ne sont pas très différents des uns des autres.			

7.6 Formule donnant la note CWSS

Une note CWSS 1.0 est comprise entre 0 et 100. Elle est calculée comme suit:

```
Sous-noteRésultatDeBase * Sous-noteSurfaceD'attaque * Sous-NoteEnvironnement
```

La Sous-noteRésultatDeBase prend des valeurs comprises entre 0 et 100. La Sous-noteSurfaceD'attaque et la Sous-NoteEnvironnement prennent des valeurs comprises entre 0 et 1.

7.6.1 Sous-note résultat de base

La sous-note résultat de base (Sous-noteRésultatDeBase) est calculée comme suit:

```
Base = [ (10 * ImpactTechnique + 5*(PrivilègesAcquis +
CoucheDesPrivilègesAcquis) + 5*ConfianceDansLeRésultat) * f(ImpactTechnique) *
EfficacitéDuContrôleInterne ] * 4,0
```

```
f(ImpactTechnique) = 0 si ImpactTechnique = 0; sinon f(ImpactTechnique) = 1.
```

La valeur maximale potentielle de Sous-noteRésultatDeBase est de 100.

La définition de f(ImpactTechnique) a un équivalent dans le CVSS. Elle est utilisée pour faire en sorte que si l'impact technique est égal à 0, les autres facteurs ajoutés ne génèrent pas par inadvertance une note non nulle.

L'ImpactTechnique et la combinaison PrivilègesAcquis/CoucheDesPrivilègesAcquis se voient attribuer le même poids, représentant chacun 40% de la Sous-noteRésultatDeBase. (Chacun génère une sous-valeur égale au maximum à 10). Un ajustement est opéré en fonction de la confiance dans le résultat, qui représente 20% de la base (maximum de 5). L'EfficacitéDuContrôleInterne peut abaisser la note, éventuellement jusqu'à 0, selon la puissance des contrôles internes éventuellement appliqués. Après application de l'EfficacitéDuContrôleInterne, l'intervalle possible de résultats est compris entre 0 et 25, de sorte qu'on utilise un coefficient de 4,0 pour que l'intervalle de la Sous-noteRésultatDeBase soit compris entre 0 et 100.

7.6.2 Sous-note surface d'attaque

La Sous-noteSurfaceD'attaque est calculée comme suit:

```
[  20*(PrivilègesRequis + CoucheDesPrivilègesRequis + VecteurD'accès) +
20*DomaineDeDéploiement + 15*NiveauD'interaction + 5*PuissanceD'authentification
] / 100,0
```

La combinaison des privilèges requis/accès représente 60% de la sous-note surface d'attaque; le domaine de déploiement, 20% supplémentaires; l'interaction, 15%; et l'authentification, 5%. On ne donne pas beaucoup d'importance aux exigences d'authentification, car on suppose qu'une preuve d'identité puissante ne dissuadera pas de manière significative un attaquant de tenter d'exploiter la vulnérabilité.

On obtient ainsi un intervalle de valeurs comprises entre 0 et 100, que l'on divise ensuite par 100.

7.6.3 Sous-note environnemement

La Sous-noteEnvironnement est calculée comme suit:

```
[ (10*ImpactSurLesActivités + 3*ProbabilitéDeDécouverte + 4*ProbabilitéD'exploit
+ 3*Prévalence) * f(ImpactSurLesActivités) * EfficacitéDuContrôleExterne ] /
20,0
```

```
f(ImpactSurLesActivités) = 0 si ImpactSurLesActivités == 0; sinon
f(ImpactSurLesActivités) = 1
```

L'ImpactSurLesActivités représente 50% de la note environnement, et il peut ramener la note finale à 0. L'EfficacitéDuContrôleExterne est toujours non nul (pour tenir compte du risque qu'il puisse être supprimé par inadvertance en cas de modification de l'environnement), et peut avoir une grande incidence sur la note finale. La combinaison de la ProbabilitéDeDécouverte et de la ProbabilitéD'exploit représente 35% de la note et la Prévalence 15%.

7.6.4 Autres éléments concernant la formule

Il existe une grande diversité des types de notes qui peuvent être représentés, même si la multiplication de nombreux facteurs différents, associée à de multiples poids ayant de faibles valeurs, a tendance à déplacer l'intervalle des notes potentielles vers les valeurs les plus faibles.

Étant donné que les valeurs "non applicable" ont un poids de 1, la formule donne toujours une note maximale potentielle de 100,0. Dans les cas extrêmement rares dans lesquels certains facteurs sont considérés comme non applicables (par exemple impact technique, impact sur les activités *et* efficacité du contrôle interne), la note minimale possible pourrait être non nulle.

Lorsque, pour une note donnée, on utilise les valeurs par défaut pour un grand nombre de facteurs, à savoir les poids médians tels que définis dans le CWSS 1.0, les notes auront largement tendance à être déplacées vers les valeurs faibles. Le poids médian pour un facteur ne reflète pas nécessairement la valeur la plus probable qui puisse être utilisée, de sorte que le choix des poids correspondant aux valeurs par défaut pourra être modifié dans de futures versions. Dans l'idéal, la formule aurait comme propriété que l'utilisation de nombreuses valeurs par défaut conduit à une note relativement proche de 50; le choix de valeurs autres que les valeurs par défaut devrait avoir pour effet d'ajuster la note finale vers le haut ou vers le bas, permettant ainsi d'augmenter la précision.

De même, en cas d'utilisation de valeurs "inconnu", les notes auront généralement tendance à être déplacées vers les valeurs faibles. Ce peut être utile, car les notes seront plus élevées si on dispose d'informations plus spécifiques.

7.7 Vecteurs CWSS, exemples de notation et portabilité de la note

L'utilisation des codes spécifiés pour chaque facteur permet de stocker une note CWSS sous une forme compacte, analysable automatiquement et lisible par l'homme qui décrit en détail la manière dont la note a été générée. Cette façon de procéder est très analogue à la manière dont les vecteurs CVSS sont élaborés.

A la différence du CVSS, les facteurs CWSS ne peuvent pas tous être décrits de manière symbolique avec des valeurs discrètes. N'importe quel facteur peut être quantifié au moyen de poids continus qui annulent et remplacent les valeurs discrètes par défaut définies au départ, en utilisant la valeur "Q". Lorsqu'il est calculé au moyen du CWRAF, le facteur d'impact est en réalité une expression incluant 32 impacts techniques et couches distincts, parmi lesquels un grand nombre ne s'appliqueraient pas à une faille particulière. Traiter chaque impact comme un facteur distinct aurait approximativement pour effet de doubler le nombre de facteurs nécessaires pour calculer une note CWSS. De plus, l'utilisation par le CWRAF d'un contexte de valeur des activités (BVC) pour ajuster les notes en fonction des préoccupations propres aux activités signifie aussi qu'une note CWSS et son vecteur peuvent sembler incohérents s'ils sont "transportés" dans d'autres domaines ou vignettes.

Cela étant, un vecteur CWSS 1.0 devrait indiquer explicitement le poids utilisé pour chaque facteur, même s'il s'ensuit une augmentation de la taille du vecteur.

Le format d'un facteur donné dans un vecteur CWSS est le suivant:

NomDufacteur: Valeur, Poids

Par exemple, "`P:NA,1,0`" correspond à la valeur "non applicable" pour la prévalence avec un poids de 1,0. "`AV:P,0,2`" correspond à la valeur "physique" pour le vecteur d'accès avec un poids de 0,2.

Les facteurs sont séparés par une barre oblique, par exemple:

```
AV:I,1,0/RP:G,0,9/AS:N,1,0
```

donne la liste des valeurs et des poids pour "AV" (vecteur d'accès), "RP" (couche des privilèges requis) et "AS" (puissance d'authentification).

Si un vecteur CWSS n'indique pas le poids réel correspondant à une valeur, une mise en oeuvre devrait signaler une éventuelle erreur ou incohérence, tenter de déduire la version du CWSS à partir des facteurs du vecteur et de leurs valeurs, recalculer la note CWSS sur la base de la version déduite, et comparer cette note à la note d'origine. Si les notes sont incohérentes, la mise en oeuvre devrait signaler une éventuelle erreur ou incohérence.

7.7.1 Exemple: application critique pour les activités de l'entreprise

Considérons le cas d'une faille dans une application qui constitue la principale source de recettes pour une société, et qui a donc une valeur critique pour les activités de l'entreprise. L'application permet à des internautes arbitraires d'ouvrir un compte en utilisant uniquement une adresse électronique. Un utilisateur peut ensuite exploiter la faille pour obtenir les privilèges administrateur pour l'application, mais l'attaque ne peut aboutir que lorsque l'administrateur obtient un rapport des activités récentes des utilisateurs – chose courante. L'attaquant ne peut pas prendre le contrôle complet de l'application, mais il peut supprimer ses utilisateurs et données. Supposons en outre qu'il n'existe pas de contrôles pour éviter la faille, mais qu'il est facile de résoudre le problème, et que seules quelques lignes de code sont nécessaires.

Cette situation pourrait être représentée par le vecteur CWSS suivant:

```
(TI:H,0,9/AP:A,1,0/AL:A,1,0/IC:N,1,0/FC:T,1,0/
RP:G,0,9/RL:A,1,0/AV:I,1,0/AS:N,1,0/IN:T,0,9/SC:A,1,0/
BI:C/0,9,DI:H,1,0/EX:H,1,0/EC:N,1,0/P:NA,1,0)
```

Le vecteur est écrit sur plusieurs lignes dans un souci de lisibilité, chaque ligne correspondant à un groupe de métriques.

Les facteurs et leurs valeurs sont tels qu'indiqués dans le Tableau 19, ci-après.

Tableau 19 – Facteurs et valeurs dans le cas d'une application critique pour les activités de l'entreprise

Facteur	Valeur
Impact technique	Élevé
Privilèges acquis	Administrateur
Couche des privilèges acquis	Application
Efficacité du contrôle interne	Aucun
Confiance dans le résultat	Véridique
Privilèges requis	Invité
Couche des privilèges requis	Application
Vecteur d'accès	Internet
Puissance d'authentification	Aucun
Niveau d'interaction	Type/Limité
Domaine de déploiement	Tous
Impact sur les activités	Critique
Probabilité de découverte	Élevé
Probabilité d'exploit	Élevé
Efficacité du contrôle externe	Aucun
Prévalence	NA

La note CWSS pour ce vecteur est de 92,6, calculée comme suit:

- Sous-noteDeBase:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4,0`
  - `f(TI) = 1`
  - `= [ (10 * 0,9 + 5*(1,0 + 1,0) + 5*1,0) * 1 * 1,0 ] * 4,0`
  - `= [ (9,0 + 10,0 + 5,0) * 1,0 ] * 4,0`

- = 24,0 * 4,0
- = 96,0

- Sous-noteSurfaceD'attaque:
  - [20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS] / 100,0
  - = [20*(0,9 + 1,0 + 1,0) + 20*1,0 + 15*0,9 + 5*1,0] / 100,0
  - = [58,0 + 20,0 + 13,5 + 5,0] / 100,0
  - = 96,5 / 100,0
  - = 0,965
- Sous-noteEnvironnement:
  - [(10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC] / 20,0
  - f(BI) = 1
  - = [(10*1,0 + 3*1,0 + 4*1,0 + 3*1,0) * 1 * 1,0] / 20,0
  - = [(10,0 + 3,0 + 4,0 + 3,0) * 1,0] / 20,0
  - = 20,0 / 20,0
  - = 1,0.

La note finale est:

96,0 * 0,965 * 1,0 = 92,64 == 92,6

7.7.2 Exemple: wiki à criticité limitée pour les activités de l'entreprise

Considérons le vecteur CWSS ci-après. Supposons que le logiciel est un wiki qui est utilisé pour rechercher les réceptions pour une moyenne entreprise. Parmi les caractéristiques les plus importantes, l'impact technique est moyen pour un utilisateur normal de l'application qui devient administrateur, mais l'application n'est pas critique pour les activités de l'entreprise, de sorte que l'impact global sur les activités est faible. Il convient par ailleurs de noter que la plupart des facteurs de l'environnement sont mis à "non applicable."

(TI:M,0,6/AP:A,1,0/AL:A,1,0/IC:N,1,0/FC:T,1,0/

RP:RU,0,7/RL:A,1,0/AV:I,1,0/AS:W,0,9/IN:A,1,0/SC:NA,1,0/

BI:L/0,3,DI:NA,1,0/EX:NA,1,0/EC:N,1,0/RE:NA,1,0/P:NA,1,0)

Le vecteur est écrit sur plusieurs lignes dans un souci de lisibilité, chaque ligne correspondant à un groupe de métriques.

Les facteurs et leurs valeurs sont tels qu'indiqués dans le Tableau 20, ci-après.

Tableau 20 – Facteurs et valeurs dans le cas d'une application à criticité limitée pour les activités de l'entreprise

Facteur	Valeur
Impact technique	Moyen
Privilèges acquis	Administrateur
Couche des privilèges acquis	Application
Efficacité du contrôle interne	Aucun
Confiance dans le résultat	Véridique
Privilèges requis	Utilisateur normal
Couche des privilèges requis	Application
Vecteur d'accès	Internet
Puissance d'authentification	Faible
Niveau d'interaction	Automatique
Domaine de déploiement	NA
Impact sur les activités	Faible
Probabilité de découverte	NA
Probabilité d'exploit	NA
Efficacité du contrôle externe	Aucun
Prévalence	NA

La note CWSS pour ce vecteur est de 51,1, calculée comme suit:

- Sous-noteDeBase:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4,0`
  - `f(TI) = 1`
  - `= [ (10 * 0,6 + 5*(1 + 1) + 5*1) * f(TI) * 1 ] * 4,0`
  - `= 84,0`
- Sous-noteSurfaceD'attaque:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100,0`
  - `= [ 20*(0,7 + 1 + 1) + 20*1,0 + 15*1,0 + 5*0,9 ] / 100,0`
  - `= [ 54,0 + 20,0 + 15,0 + 4,5 ] / 100,0`
  - `= 93,5 / 100,0`
  - `= 0,94 (0,935)`
- Sous-noteEnvironnement:
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20,0`
  - `f(BI) = 1`
  - `= [ (10*0,3 + 3*1,0 + 4*1,0 + 3*1,0) * f(BI) * 1 ] / 20,0`
  - `= [ (3,0 + 3,0 + 4,0 + 3,0) * 1,0 * 1,0 ] / 20,0`
  - `= [ 13,0 * 1,0 ] / 20,0`
  - `= 0,65.`

La note finale est:

`84,0 * 0,935 * 0,65 = 51,051 == 51,1`

7.7.3 Autres approches concernant la portabilité de la note CWSS

Au lieu d'inclure les différents poids dans un vecteur CWSS, plusieurs autres méthodes pourraient être adoptées.

L'une des possibilités consiste à étendre les vecteurs CWSS afin d'inclure des métadonnées supplémentaires qui n'ont pas d'incidence sur la note mais rendent compte de la version ou d'autres informations importantes. La partie relative aux métadonnées n'aurait pas nécessairement besoin d'indiquer les poids proprement dits. Par exemple, la version du CWSS pourrait être indiquée en utilisant un nom de "facteur" tel que "V" conjointement avec une valeur qui représente la version du CWSS, par exemple "V:1.1", ce qui ajouterait environ 4 octets à chaque vecteur CWSS. Dans ce cas, si la version est codée dans un vecteur, il ne serait plus nécessaire d'indiquer les poids attribués (sauf pour les valeurs quantifié), de sorte que les vecteurs résultants pourraient être beaucoup plus courts.

Une approche différente consisterait à joindre des métadonnées à un ensemble de notes CWSS générées (comme la fiche de notation de l'impact technique en cas d'utilisation du CWRAF), mais ces métadonnées pourraient se détacher trop facilement des notes/vecteurs. Quant aux facteurs quantifiés, il serait toujours nécessaire de les représenter dans un vecteur, car ils pourraient varier en fonction du résultat signalant une faille.

Selon une autre approche encore, lorsque les notes CWSS sont transférées d'une partie à une autre, la partie qui les reçoit pourrait recalculer les notes à partir des vecteurs CWSS donnés, puis comparer les notes recalculées avec les notes d'origine. Une différence entre les notes laisserait supposer que les parties utilisent des mécanismes différents, éventuellement une version différente du CWSS.

Bibliographie

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

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

[b-UIT-T X.1521] Recommandation UIT-T X.1521 (2011), *Système d'évaluation des vulnérabilités courantes*.

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Liste des failles courantes*.

[b-UIT-T X.1544] Recommandation UIT-T X.1544 (2013), *Liste et classification des schémas d'attaque courants*.

[b-CWRAF] Common Weakness Risk Analysis Framework, http://cwe.mitre.org/cwraf/.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020