Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1521

(03/2016)

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

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

Système d'évaluation des vulnérabilités courantes version 3.0

Recommandation UIT-T X.1521

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

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

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

Recommandation UIT-T X.1521

Système d'évaluation des vulnérabilités courantes version 3.0

Résumé

La Recommandation UIT-T X.1521, qui porte sur le système d'évaluation des vulnérabilités courantes (CVSS, *common vulnerability scoring system*), définit un cadre ouvert pour la communication des caractéristiques et des incidences des vulnérabilités en matière de technologies de l'information et de la communication (TIC) rencontrées dans les logiciels commerciaux ou libres utilisés dans les réseaux de communication, dans les dispositifs d'utilisateur final, ou dans tout autre type de dispositif TIC capable d'utiliser des logiciels. L'objectif de cette Recommandation est de permettre aux gestionnaires des TIC, aux fournisseurs de bulletins d'information sur les vulnérabilités, aux fournisseurs de systèmes de sécurité, aux fournisseurs d'applications et aux chercheurs d'utiliser un langage commun en ce qui concerne l'évaluation des vulnérabilités en matière de TIC.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1521	2011-04-20	17	11.1002/1000/11062
2.0	ITU-T X.1521	2016-03-23	17	11.1002/1000/12614

Mots clés

CVSS, CYBEX, mesures, système d'évaluation des vulnérabilités courantes.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
3.1	Terme défini ailleurs	1
3.2	Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes	2
5	Conventions	3
6	Système d'évaluation des vulnérabilités courantes	3
6.1	Introduction	3
6.2	Mesures de base	6
6.3	Mesures temporelles	11
6.4	Mesures environnementales	13
6.5	Echelle de notation qualitative de la gravité	15
6.6	Chaîne vectorielle	16
6.7	Définition du schéma XML CVSS version 3.0	17
6.8	Equations CVSS version 3.0	17
Appendice I – Manuel d'utilisation du système CVSS version 3.0		21
I.1	Introduction	21
I.2	Modifications apportées au système CVSS version 3.0	21
I.2.1	Champ, composante vulnérable et composante touchée	22
I.2.2	Vecteur de l'attaque	23
I.2.3	Complexité de l'attaque	23
I.2.4	Privilèges requis	23
I.2.5	Mesures des incidences	24
I.2.6	Mesures temporelles	24
I.2.7	Mesures environnementales	24
I.2.8	Echelle de notation qualitative	24
I.2.9	Synthèse des modifications	24
I.3	Orientations en matière d'évaluation	25
I.3.1	Evaluation CVSS dans le cycle de vie de l'exploitation d'une vulnérabilité	25
I.3.2	Incidences en matière de confidentialité et d'intégrité comparées aux incidences en matière de disponibilité	26
I.3.3	Vulnérabilités locales exploitées par des attaquants distants	26
I.3.4	Vulnérabilités résultant de l'exécution d'un script intersites	27
I.3.5	Intercepteur	27
I.3.6	Vulnérabilités matérielles	27
I.3.7	Enchaînement de vulnérabilités	27
I.4	Glossaire	28

Page

I.5 Rubrique sur l'évaluation 29
I.5.1 Vecteur de l'attaque 29
I.5.2 Complexité de l'attaque 30
I.5.3 Privilèges requis 30
I.5.4 Intervention de l'utilisateur 30
I.5.5 Champ 30
I.5.6 Incidences en matière de confidentialité 31
I.5.7 Incidences en matière d'intégrité 31
I.5.8 Incidences en matière de disponibilité 31
Appendice II – Ressources et liens 32
Bibliographie 33

Introduction

Le système d'évaluation des vulnérabilités courantes (CVSS, *common vulnerability scoring system*) définit un cadre ouvert pour la communication des caractéristiques et de la gravité des vulnérabilités logicielles. Le système CVSS comporte trois groupes de mesures: le groupe de mesures de base, le groupe de mesures temporelles et le groupe de mesures environnementales. Le groupe de mesures de base concerne les propriétés intrinsèques d'une vulnérabilité, le groupe de mesures temporelles vise les caractéristiques d'une vulnérabilité qui évoluent dans le temps, et le groupe de mesures environnementales se rapporte aux particularités d'une vulnérabilité qui sont propres à l'environnement d'un utilisateur. Les mesures de base permettent d'attribuer une note comprise entre 0 et 10, qui peut ensuite être modifiée par la notation des mesures temporelles et environnementales. Une note CVSS est aussi représentée par une chaîne vectorielle, qui est une représentation textuelle comprimée des valeurs employées pour obtenir la note. La présente Recommandation contient la spécification officielle du système CVSS version 3.0.

Le système CVSS version 3.0 apporte des améliorations en profondeur au système CVSS version 2.0 mais n'est pas compatible avec lui. Lors de l'utilisation du système CVSS version 2.0, plusieurs points faibles de cette spécification sont apparus. Parmi eux, on peut citer: l'évaluation des vulnérabilités dans un environnement virtuel, notamment les vulnérabilités "indirectes" telles que celles qui résultent de l'exécution d'un script intersites, ou l'impossibilité de tenir compte des interdépendances entre les applications dans un même système ou de tenir compte des actions d'un utilisateur autre que l'attaquant. De plus amples informations sur les améliorations de la version 3.0 sont données au § 2 de l'Appendice I.

En s'attaquant à ces points faibles, le groupe de travail CVSS s'est rendu compte qu'il n'était pas possible d'assurer la compatibilité avec le système CVSS version 2.0. Tout en reconnaissant que l'absence de compatibilité pourrait poser des problèmes pour les systèmes existants qui emploient et exploitent le système CVSS version 2.0, nous sommes d'avis que la version 3.0 offre un intérêt suffisant pour compenser cet inconvénient. Nous conseillons fortement aux fabricants et aux utilisateurs qui produisent et exploitent le système CVSS version 2.0 de passer au système CVSS version 3.0.

Même si la spécification CVSS version 2.0 continuera d'être disponible pour des raisons historiques, elle ne sera plus en vigueur. Les responsables chargés de la mise en oeuvre d'outils et de méthodes sont vivement encouragés à adopter la spécification CVSS version 3.0 tout en continuant à prendre en charge la version 2.0 afin de traiter les vulnérabilités existantes qui ont déjà été notées à l'aide de la spécification CVSS version 2.0.

Recommandation UIT-T X.1521

Système d'évaluation des vulnérabilités courantes version 3.0

1 Domaine d'application

La présente Recommandation décrit une approche normalisée pour la communication des caractéristiques et des incidences des vulnérabilités, s'agissant des technologies de l'information et de la communication (TIC), au moyen de mesures temporelles et environnementales qui emploient des informations contextuelles afin de rendre compte plus précisément des risques pour l'environnement propre à chaque utilisateur.

La présente Recommandation est techniquement équivalente et compatible avec le "système d'évaluation des vulnérabilités courantes (CVSS) version 3", daté du 10 juin 2015, qui figure sur le site web à l'adresse http://www.first.org/cvss.

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. Toutes 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 Terme défini ailleurs

La présente Recommandation emploie le terme suivant défini ailleurs:

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

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 accès: l'aptitude d'un sujet à visualiser ou à modifier un objet ou à communiquer avec celui-ci. L'accès rend le flux d'informations entre le sujet et l'objet possible.

3.2.2 disponibilité: la fourniture d'un accès fiable et en temps utile aux données et aux ressources par des personnes autorisées.

3.2.3 confidentialité: un principe de sécurité qui vise à garantir que les informations ne soient pas divulguées à des sujets non autorisés.

3.2.4 intégrité: un principe de sécurité qui garantit que les informations et les systèmes ne sont pas modifiés de façon malveillante ou accidentelle.

3.2.5 risques: les incidences relatives sur un environnement d'utilisateur pouvant résulter de l'exploitation d'une faille.

3.2.6 menace: la probabilité ou la fréquence de production d'un événement préjudiciable.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

A incidences en matière de disponibilité (*availability impact*)
AC complexité de l'attaque (*attack complexity*)
AR exigence de disponibilité (*availability requirement*)
ARP protocole de résolution d'adresse (*address resolution protocol*)
AV vecteur de l'attaque (*attack vector*)
C incidences en matière de confidentialité (*confidentiality impact*)
CIA confidentialité, intégrité et disponibilité (*confidentiality, integrity, and availability*)
CPU unité centrale de traitement (*central processing unit*)
CR exigence de confidentialité (*confidentiality requirement*)
CVE vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)
CVSS système d'évaluation des vulnérabilités courantes (*common vulnerability scoring system*)
CWE liste des failles courantes (*common weakness enumeration*)
DMA accès direct à la mémoire (*direct memory access*)
DNS système de noms de domaine (*domain name system*)
DOM modèle objet de documents (*document object model*)
DoS déni de service (*denial-of-service*)
E maturité du code d'exploitation (*exploit code maturity*)
I incidences en matière d'intégrité (*integrity impact*)
ID identificateur (*identifier*)
IP protocole Internet (*Internet protocol*)
IR exigence d'intégrité (*integrity requirement*)
ISC note partielle des incidences (*impact sub score*)
IT technologie informatique (*information technology*)
LAN réseau local (*local area network*)
MA disponibilité modifiée (*modified availability*)
MAC complexité de l'attaque modifiée (*modified attack complexity*)
MAV vecteur de l'attaque modifié (*modified attack vector*)
MC confidentialité modifiée (*modified confidentiality*)
MI intégrité modifiée (*modified integrity*)
MPR privilèges requis modifiés (*modified privileges required*)
MS champ modifié (*modified scope*)
MUI intervention de l'utilisateur modifiée (*modified user interaction*)
NIST National Institute of Standards and Technology
OS système d'exploitation (*operating system*)
OSI interconnexion des systèmes ouverts (*open systems interconnection*)
PCI DSS Payment Card Industry Data Security Standard

PR privilèges requis (*privileges required*)

RC confiance indiquée (*report confidence*)

RL niveau de correction (*remediation level*)

RPC invocation de procédure à distance (*remote procedure call*)

S champ (*scope*)

SCAP Security Content Automation Protocol

SQL langage de requête structuré (*structured query language*)

TCP protocole de commande de transmission (*transmission control protocol*)

TIC technologies de l'information et de la communication

UI intervention de l'utilisateur (*user interaction*)

USB bus série universel (*universal serial bus*)

VM machine virtuelle (*virtual machine*)

XSS exécution d'un script intersites (*cross site scripting*)

5 Conventions

Aucune.

6 Système d'évaluation des vulnérabilités courantes

Le système d'évaluation des vulnérabilités courantes (CVSS) définit un cadre ouvert pour la communication des caractéristiques et de la gravité des vulnérabilités logicielles. Le système CVSS comporte trois groupes de mesures: le groupe de mesures de base, le groupe de mesures temporelles et le groupe de mesures environnementales. Le groupe de mesures de base concerne les propriétés intrinsèques d'une vulnérabilité, le groupe de mesures temporelles vise les caractéristiques d'une vulnérabilité qui évoluent dans le temps, et le groupe de mesures environnementales se rapporte aux particularités d'une vulnérabilité qui sont propres à l'environnement d'un utilisateur. Les mesures de base permettent d'attribuer une note comprise entre 0 et 10, qui peut ensuite être modifiée par la notation des mesures temporelles et environnementales. Une note CVSS est aussi représentée par une chaîne vectorielle, qui est une représentation textuelle comprimée des valeurs employées pour obtenir la note. La présente Recommandation contient la spécification officielle du système CVSS version 3.0.

6.1 Introduction

Les vulnérabilités logicielles, matérielles et micrologicielles présentent des risques sérieux pour les entreprises qui exploitent un réseau informatique, et elles peuvent être difficiles à classer et à réduire. Le système d'évaluation des vulnérabilités courantes (CVSS) est un moyen qui permet de déterminer les principales caractéristiques d'une vulnérabilité, d'obtenir une note chiffrée rendant compte de sa gravité, et de donner une représentation textuelle de cette note. La note chiffrée peut être traduite sur le plan qualitatif (degré de gravité faible, moyen, élevé ou très élevé) afin d'aider les entreprises à évaluer correctement leurs processus de gestion des vulnérabilités et à attribuer un degré de priorité à ceux-ci.

En bref, le système CVSS a trois grands avantages. D'abord, il permet d'obtenir des notes normalisées des vulnérabilités. Lorsqu'une entreprise emploie un seul algorithme pour l'évaluation des vulnérabilités sur l'ensemble de ses plates-formes informatiques, elle peut s'appuyer sur une seule politique de gestion des vulnérabilités pour définir le temps maximal nécessaire à la confirmation et à la correction de la vulnérabilité donnée. Ensuite, le système CVSS définit un cadre ouvert. Les utilisateurs peuvent être désorientés lorsqu' une note arbitraire est attribuée à une vulnérabilité par

une entité tierce. Avec le système CVSS, les différentes caractéristiques employées pour obtenir une note sont transparentes. Enfin, le système CVSS permet d'attribuer un degré de priorité. Lorsque la note environnementale est calculée, la vulnérabilité est considérée dans le contexte propre à chaque entreprise, et cette note aide à mieux comprendre le risque que présente ladite vulnérabilité pour l'entreprise.

La présente Recommandation contient la spécification officielle du système CVSS version 3.

6.1.1 Mesures

Le système CVSS comporte trois groupes de mesures: le groupe de mesures de base, le groupe de mesures temporelles et le groupe de mesures environnementales, chacun d'eux renfermant un ensemble de mesures, comme illustré dans la Figure 1.

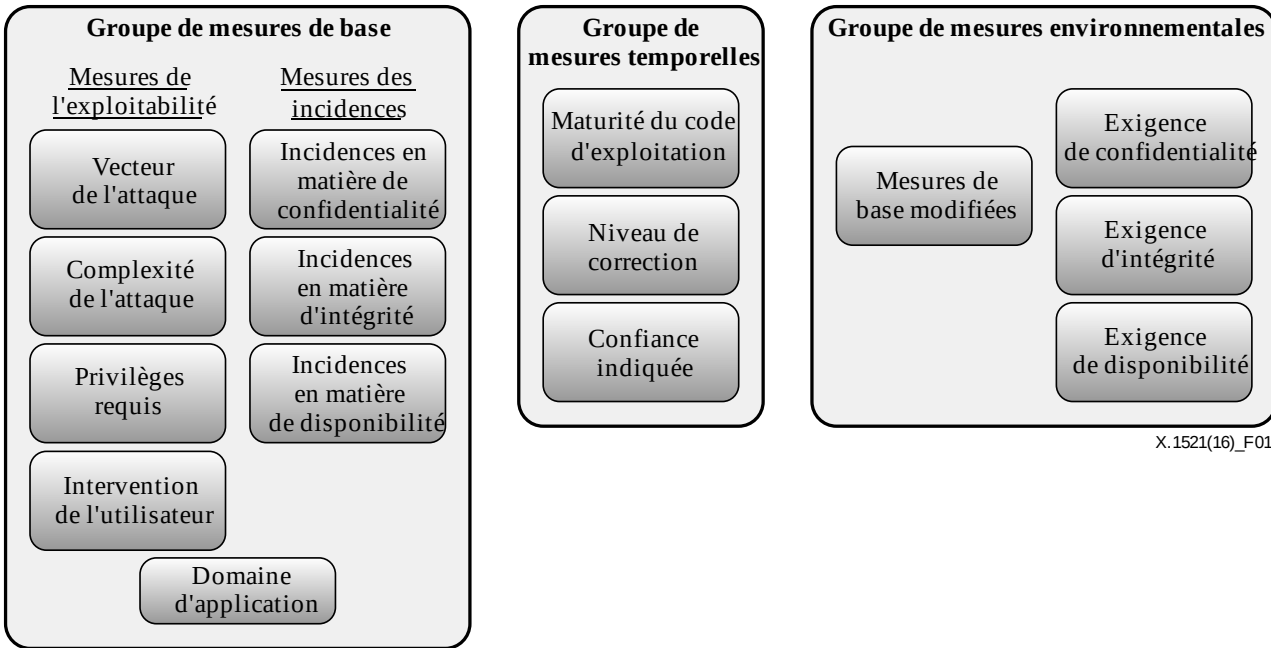


Figure 1 – Les groupes de mesures du système CVSS version 3.0

Le groupe de mesures de base concerne les caractéristiques intrinsèques d'une vulnérabilité qui sont indépendantes du temps et des environnements d'utilisateurs. Il renferme deux ensembles de mesures: les mesures de l'exploitabilité et les mesures des incidences.

Les mesures de l'exploitabilité correspondent à la facilité et aux moyens techniques qui peuvent être employés pour exploiter les failles. C'est-à-dire, elles rendent compte des caractéristiques de l'*objet vulnérable*, que nous nommons de façon formelle la *composante vulnérable*. Et en parallèle, les mesures des incidences correspondent à la conséquence directe d'une exploitation réussie, et rendent compte de la conséquence pour l'*objet touché*, que nous nommons de façon formelle la *composante touchée*.

Tandis que la composante vulnérable est en général une application logicielle, un module, un pilote, etc. (ou éventuellement un dispositif matériel), la composante touchée peut être une application logicielle, un dispositif matériel ou une ressource de réseau. Cette aptitude à mesurer les incidences d'une vulnérabilité sur un objet autre que la composante vulnérable est une caractéristique essentielle du système CVSS version 3.0. Cette propriété est prise en compte et examinée plus en détail dans le cadre de la mesure "champ" ci-dessous.

Le groupe de mesures temporelles concerne les caractéristiques d'une vulnérabilité qui peuvent évoluer dans le temps mais n'évoluent pas d'un environnement d'utilisateur à un autre. Par exemple, la note CVSS augmentera en présence d'un kit d'exploitation simple à utiliser mais diminuera lorsqu'un correctif officiel est employé.

Le groupe de mesures environnementales concerne les caractéristiques d'une vulnérabilité qui sont pertinentes et propres à un environnement d'utilisateur particulier. Ces mesures permettent aux analystes chargés de l'évaluation d'intégrer des commandes de sécurité qui peuvent atténuer les conséquences, d'une part, et, d'autre part, accroître ou diminuer l'importance d'un système vulnérable en fonction des risques qu'il présente pour l'entreprise.

Chacune de ces mesures est examinée plus en détail ci-après.

6.1.2 Notation

Lorsqu'un analyste a défini les valeurs des mesures de base, l'équation de base permet de calculer une note comprise entre 0,0 et 10,0, comme illustré dans la Figure 2.

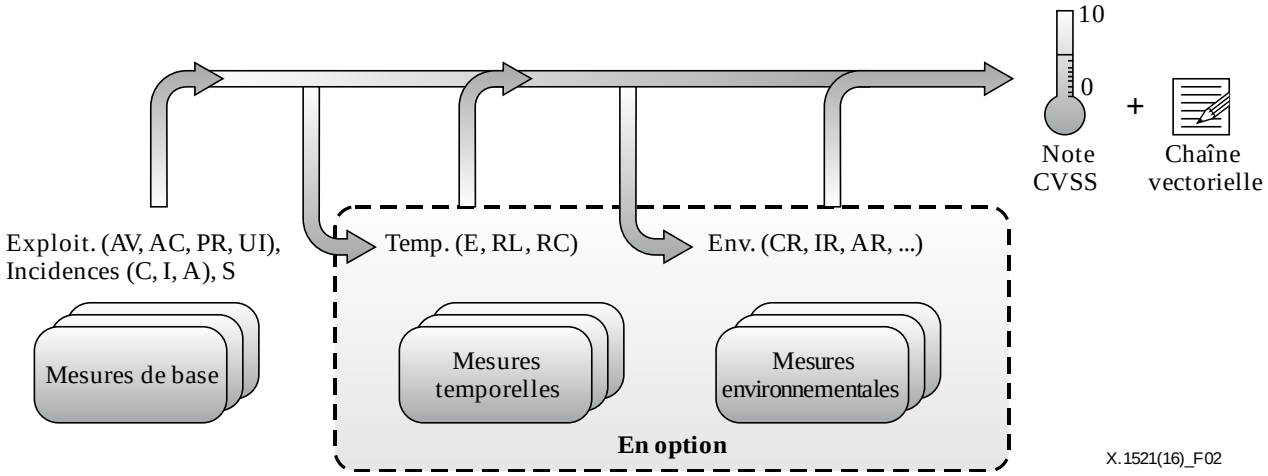


Figure 2 – Mesures et équations CVSS

Concrètement, l'équation de base est obtenue à partir de deux sous-équations, l'équation de la note partielle de l'exploitabilité et l'équation de la note partielle des incidences. L'équation de la note partielle de l'exploitabilité est obtenue à partir de la mesure de l'exploitabilité de base, tandis que l'équation de la note partielle des incidences est obtenue à partir des mesures des incidences de base.

La note de base peut ensuite être affinée au moyen de la notation des mesures temporelles et environnementales de manière à rendre plus précisément compte des risques présentés par une vulnérabilité pour un environnement d'utilisateur donné. Mais la notation des mesures temporelles et environnementales n'est pas obligatoire.

En général, les mesures de base et les mesures temporelles sont définies par les analystes chargés des bulletins d'information sur les vulnérabilités, les fabricants de systèmes de sécurité ou les éditeurs d'applications, parce ce que ce sont eux qui possèdent habituellement les informations les plus précises sur les caractéristiques d'une vulnérabilité. Quant aux mesures environnementales, elles sont définies par les entreprises utilisatrices finales parce que ce sont elles qui sont le mieux à même d'évaluer les incidences potentielles d'une vulnérabilité dans leur propre environnement informatique.

La notation des mesures CVSS permet aussi d'obtenir une chaîne vectorielle, à savoir une représentation textuelle des valeurs de mesure, employées pour obtenir la note de la vulnérabilité. Cette chaîne vectorielle est une chaîne textuelle spécifiquement formatée qui contient les valeurs de mesure et qui devrait toujours s'afficher, accompagnée de la note de la vulnérabilité.

Les équations d'évaluation et les chaînes vectorielles sont décrites plus en détail ci-après.

Il convient d'observer que la notation de l'ensemble des mesures devrait se faire en supposant que l'attaquant a déjà localisé et identifié la vulnérabilité. L'analyste n'a donc pas besoin de prendre en compte les moyens à l'aide desquels la vulnérabilité a été identifiée. Par ailleurs, il est probable que diverses personnes procèderont à l'évaluation des vulnérabilités (par exemple, les éditeurs de logiciels, les analystes chargés des bulletins d'information sur les vulnérabilités, les fabricants de systèmes de sécurité, etc.), mais il convient toutefois de noter que l'évaluation des vulnérabilités est conçue pour être indépendante de ces personnes et de leurs entreprises.

6.2 Mesures de base

6.2.1 Mesures de l'exploitabilité

Comme mentionné, les mesures de l'exploitabilité rendent compte des caractéristiques de l'*objet vulnérable*, que nous nommons de façon formelle la *composante vulnérable*. En raison de cela, chacune des mesures de l'exploitabilité énumérées ci-après devrait être notée par rapport à la composante vulnérable, et rendre compte des propriétés de la vulnérabilité qui permettraient qu'une attaque réussisse.

6.2.1.1 Vecteur de l'attaque (AV)

Cette mesure rend compte du contexte qui rend possible l'exploitation de la vulnérabilité. La valeur de la mesure (et par conséquent la note de base) sera d'autant plus grande que l'attaquant est loin (en termes de distance logique et physique) de la composante vulnérable qu'il attaque. On suppose que le nombre d'attaquants potentiels, s'agissant d'une vulnérabilité qui pourrait être exploitée à travers l'ensemble du réseau Internet, est supérieur au nombre d'attaquants potentiels qui pourraient exploiter une vulnérabilité nécessitant un accès physique à un dispositif, ce qui conduit à une note plus élevée dans le premier cas. La liste des valeurs possibles est présentée dans le Tableau 1.

Tableau 1 – Vecteur de l'attaque

Valeur de la mesure	Description
Réseau (N)	Une vulnérabilité exploitable par le biais d'un accès au réseau signifie que la composante vulnérable est liée à la pile du réseau et que le trajet de l'attaquant se fait par l'intermédiaire de la couche 3 (la couche réseau) du modèle d'interconnexion des systèmes ouverts (OSI). Une telle vulnérabilité est souvent nommée "exploitable à distance". Elle peut être considérée comme étant exploitable à une distance d'un ou de plusieurs bonds dans le réseau (par exemple, dans la couche 3, à travers les frontières des routeurs). Un exemple d'attaque par l'intermédiaire du réseau est celle d'un attaquant qui provoque un déni de service (DoS) en envoyant un paquet spécialement conçu dans le cadre du protocole de commande de transmission (TCP) à travers l'Internet public (par exemple, la vulnérabilité CVE-2004-0230).
Réseau adjacent (A)	Une vulnérabilité exploitable par le biais d'un accès à un réseau adjacent signifie que la composante vulnérable est liée à la pile du réseau, mais que l'attaque se limite au même réseau partagé physique (par exemple, Bluetooth, IEEE 802.11) ou logique (par exemple, un sous-réseau local employant le protocole Internet (IP)) et qu'elle ne peut pas se faire à travers la frontière (par exemple, d'un routeur) dans la couche 3 du modèle OSI. Un exemple d'attaque par l'intermédiaire d'un réseau adjacent est l'inondation dans le cadre du protocole de résolution d'adresse (ARP) (IPv4) ou du protocole de découverte des voisins (IPv6) qui provoque un déni de service sur le segment du réseau local (LAN). Voir aussi la vulnérabilité CVE-2013-6014.

Tableau 1 – Vecteur de l'attaque

Valeur de la mesure	Description
Accès local (L)	Une vulnérabilité exploitable par le biais d'un accès local signifie que la composante vulnérable n'est pas liée à la pile du réseau et que le trajet de l'attaquant se fait par l'intermédiaire des capacités lire/écrire/exécuter. Dans certains cas, l'attaquant peut, afin d'exploiter la vulnérabilité, être connecté localement ou, à défaut, il peut s'appuyer sur l'intervention de l'utilisateur (UI) pour que celui-ci exécute un fichier malveillant.
Accès physique (P)	Une vulnérabilité exploitable par le biais d'un accès physique oblige l'attaquant à toucher physiquement la composante vulnérable ou à la manipuler. L'interaction physique peut être brève (par exemple, une attaque de la "femme de chambre malveillante"[1]) ou continue. Des exemples d'attaque sont, d'une part, l'attaque au démarrage à froid qui permet à un attaquant d'accéder aux clés de chiffrement du disque dur après avoir accédé physiquement au système, ou, d'autre part, les attaques périphériques telles que les attaques d'accès direct à la mémoire au moyen d'un bus Firewire ou d'un bus série universel (USB).

6.2.1.2 Complexité de l'attaque (AC)

Cette mesure décrit la situation, hors du contrôle de l'attaquant, qui doit exister pour pouvoir exploiter une vulnérabilité. Comme décrit ci-après, cette situation peut nécessiter la collecte d'un supplément d'informations sur la cible, sur la présence de certaines configurations du système ou sur des particularités informatiques. Il est important d'observer que la notation de cette mesure ne concerne pas les vulnérabilités dont l'exploitation nécessite des interventions de l'utilisateur (il en sera question lorsque les interventions de l'utilisateur seront abordées). La valeur de la mesure est d'autant plus grande que les attaques sont moins complexes. La liste des valeurs possibles est présentée dans le Tableau 2.

Tableau 2 – Complexité de l'attaque

Valeur de la mesure	Description
Faible (L)	Des conditions d'accès spécifiques ou des techniques d'atténuation n'existent pas. Un attaquant peut espérer renouveler avec succès ses attaques contre la composante vulnérable.
Grande (H)	La réussite de l'attaque dépend de circonstances échappant au contrôle de l'attaquant. Ce qui veut dire que la réussite de l'attaque ne sera pas immédiate, et que l'attaquant devra fournir un certain effort de préparation ou d'exécution, ciblant la composante vulnérable, avant de pouvoir envisager la réussite de l'attaque[2]. La réussite d'une attaque peut, par exemple, dépendre du fait que l'attaquant est en mesure de mener l'une quelconque des actions suivantes: • L'attaquant doit procéder à la reconnaissance de la cible, en ce qui concerne par exemple sa configuration, les numéros de séquence, les secrets partagés, etc. • L'attaquant doit préparer l'environnement de la cible pour rendre l'exploitation plus fiable, par exemple, en reproduisant l'exploitation pour gagner une course, ou en surmontant des techniques évoluées d'atténuation des exploitations. • L'attaquant doit se placer sur le trajet dans le réseau logique entre la cible et la ressource demandée par la victime, afin de lire et/ou de modifier les communications dans le réseau (par exemple, l'attaque par intercepteur).

1 Voir le site https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html pour une description de l'attaque de la "femme de chambre malveillante" (*evil maid attack*).

2 Il convient de noter que nous ne précisons pas la quantité des efforts nécessaires. Nous estimons simplement qu'un certain effort supplémentaire doit être fourni afin de pouvoir exploiter la vulnérabilité.

6.2.1.3 Privilèges requis (PR)

Cette mesure décrit le niveau des privilèges dont doit disposer l'attaquant *avant* de pouvoir exploiter avec succès la vulnérabilité. La valeur de la mesure est plus grande lorsqu'aucun privilège n'est requis. La liste des valeurs possibles est présentée dans le Tableau 3.

Tableau 3 – Privilèges requis

Valeur de la mesure	Description
Aucun (N)	L'attaquant ne dispose avant l'attaque d'aucune autorisation, et donc ne cherche pas à accéder à des paramètres ou à des fichiers avant de lancer une attaque.
Limités (L)	L'attaquant dispose d'une autorisation et de privilèges (requis) qui lui permettent d'employer les capacités de base d'un utilisateur, ne pouvant normalement que modifier les paramètres et les fichiers appartenant à cet utilisateur. Autrement dit, l'attaquant disposant de privilèges limités ne peut altérer que des ressources non sensibles.
Importants (H)	L'attaquant dispose d'une autorisation et de privilèges (requis) lui conférant un contrôle important (par exemple, administratif) de la composante vulnérable, susceptible de modifier les paramètres et les fichiers de l'ensemble de la composante.

6.2.1.4 Intervention de l'utilisateur (UI)

Cette mesure rend compte du fait qu'un utilisateur, autre que l'attaquant, est obligé de participer à l'action visant à compromettre avec succès la composante vulnérable. Elle indique si la vulnérabilité peut être exploitée par l'attaquant seul, ou si un autre utilisateur (ou un processus initié par lui) doit y participer d'une certaine façon. La valeur de la mesure est la plus grande lorsqu'aucune intervention de l'utilisateur n'est requise. La liste des valeurs possibles est présentée dans le **Tableau 4**.

Tableau 4 – Intervention de l'utilisateur

Valeur de la mesure	Description
Aucune (N)	Le système vulnérable peut être attaqué sans intervention de l'utilisateur.
Requise (R)	L'utilisateur est obligé d'intervenir d'une certaine façon pour que la vulnérabilité puisse être exploitée avec succès. Une telle exploitation ne peut, par exemple, réussir que si elle a lieu au cours de l'installation d'une application par un administrateur du système.

6.2.2 Champ (S)

Une propriété importante dont rend compte le système CVSS version 3.0 est la possibilité qu'une vulnérabilité dans une composante logicielle puisse se répercuter sur des ressources qui sont en dehors de ses moyens ou de ses privilèges. Les conséquences sont représentées par la mesure "champ de l'autorisation" ou plus simplement "champ".

De façon formelle, le champ se réfère à un ensemble de privilèges définis par une autorité informatique (par exemple, une application, un système d'exploitation ou un environnement dit de "bac à sable") lorsque celle-ci octroie les accès aux ressources informatiques (par exemple, les fichiers, l'unité centrale de traitement (CPU), la mémoire, etc.). Ces privilèges sont accordés selon une méthode donnée d'identification et d'autorisation. Dans certains cas, l'autorisation peut être simple ou vaguement contrôlée sur la base de règles et de normes prédéfinies. Par exemple, dans le cas de l'acheminement du trafic Ethernet vers un commutateur de réseau, le commutateur accepte le trafic qui arrive au niveau de ses ports et a autorité pour contrôler les flux de trafic vers d'autres ports de commutateur.

Lorsque l'exploitation de la vulnérabilité d'une composante logicielle dépendant d'un champ d'autorisation, permet l'altération de ressources dépendant d'un autre champ d'autorisation, une modification de champ s'est produite.

Intuitivement, on peut penser à une modification de champ comme à une rupture d'un "bac à sable". Un exemple pourrait en être la vulnérabilité dans une machine virtuelle qui permet à un attaquant de supprimer des fichiers du système d'exploitation (OS) central (peut-être même de sa propre machine virtuelle (VM)). Dans cet exemple, il y a deux autorités distinctes, chargées des autorisations, celle qui définit et fait respecter les privilèges appliqués à la machine virtuelle et à ses utilisateurs, et celle qui définit et fait respecter les privilèges appliqués au système central dans lequel la machine virtuelle est exploitée.

Une modification de champ ne pourrait pas se produire, par exemple, avec une vulnérabilité dans un logiciel Microsoft Word qui permet à un attaquant de compromettre tous les fichiers système du système d'exploitation central, parce que c'est la même autorité qui fait respecter tant les privilèges appliqués à l'instance Word de l'utilisateur que les privilèges appliqués aux fichiers système du système d'exploitation central.

La note de base est plus grande lorsqu'une modification de champ s'est produite. La liste des valeurs possibles est présentée dans le Tableau 5.

Tableau 5 – Champ

Valeur de la mesure	Description
Non modifiée (U)	L'exploitation d'une vulnérabilité ne peut altérer que les ressources gérées par une même autorité. Dans ce cas, la composante vulnérable et la composante touchée sont une et même composante.
Modifiée (C)	L'exploitation d'une vulnérabilité peut altérer des ressources hors du champ des privilèges en matière d'accès qui s'appliquent à la composante vulnérable. Dans ce cas, la composante vulnérable et la composante touchée sont différentes.

6.2.3 Mesures des incidences

Les mesures des incidences concernent les propriétés de la composante touchée. Lorsque l'exploitation réussie d'une vulnérabilité pourrait altérer une ou plusieurs composantes, les mesures des incidences sont notées par rapport à la composante qui subirait les pires conséquences directes prévisibles d'une attaque réussie. Les analystes devraient donc restreindre les incidences et ne considérer que les conséquences raisonnables auxquelles une attaque peut conduire avec certitude.

Si une modification de champ ne s'est pas produite, les mesures des incidences devraient rendre compte des incidences en matière de confidentialité, d'intégrité et de disponibilité (CIA) sur la composante vulnérable. Mais si une modification du champ s'est produite, les mesures des incidences devraient rendre compte des incidences CIA pour la composante ayant subi les pires conséquences, soit la composante vulnérable, soit la composante touchée.

6.2.3.1 Incidences en matière de confidentialité (C)

Cette mesure quantifie les incidences d'une exploitation réussie d'une vulnérabilité sur la confidentialité des ressources d'information gérées par une composante logicielle. La confidentialité consiste à limiter l'accès aux informations et la divulgation de celles-ci à des utilisateurs autorisés seulement, ainsi qu'à empêcher l'accès ou la divulgation à des utilisateurs non autorisés. La liste des valeurs possibles est présentée dans le Tableau 6. La valeur de la mesure augmente avec les pertes subies par la composante touchée.

Tableau 6 – Incidences en matière de confidentialité

Valeur de la mesure	Description
Fortes (H)	La perte de confidentialité est totale, et toutes les ressources dans la composante touchée sont divulguées à l'attaquant. A défaut, seul l'accès à certaines informations restreintes est obtenu, mais les informations divulguées présentent un danger direct et grave. Par exemple, un attaquant s'empare du mot de passe de l'administrateur ou des clés de chiffrement privées d'un serveur web.
Faibles (L)	La perte de confidentialité est partielle. L'accès à certaines informations restreintes est obtenu, mais l'attaquant n'a aucun contrôle sur la nature des informations obtenues ni sur l'importance de la perte subie. La divulgation des informations ne cause pas de perte directe et grave à la composante touchée.
Aucune (N)	Aucune perte de confidentialité dans la composante touchée n'est observée.

6.2.3.2 Incidences en matière d'intégrité (I)

Cette mesure quantifie les incidences d'une exploitation réussie d'une vulnérabilité sur l'intégrité. L'intégrité se réfère à la fiabilité et à la véracité des informations. La liste des valeurs possibles est présentée dans le Tableau 7. La valeur de la mesure augmente avec les conséquences subies par la composante touchée.

Tableau 7 – Incidences en matière d'intégrité

Valeur de la mesure	Description
Fortes (H)	La perte d'intégrité ou de protection est totale. Par exemple, l'attaquant est en mesure de modifier certains ou tous les fichiers protégés par la composante touchée. A défaut, certains fichiers seulement sont modifiés, mais les modifications malveillantes ont des conséquences directes et graves pour la composante touchée.
Faibles (L)	La modification des données est possible, mais l'attaquant n'en contrôle pas les conséquences, ou la modification est retreinte. La modification des données n'a pas d'incidences directes et graves sur la composante touchée.
Aucune (N)	Aucune perte d'intégrité dans la composante touchée n'est observée.

6.2.3.3 Incidences en matière de disponibilité (A)

Cette mesure quantifie les incidences d'une exploitation réussie d'une vulnérabilité sur la disponibilité de la composante touchée. Tandis que les mesures des incidences en matière de confidentialité et d'intégrité s'appliquent à la perte de confidentialité ou d'intégrité des données (par exemple, les informations, les fichiers) employées par la composante touchée, la présente mesure concerne la perte de disponibilité de la composante touchée elle-même, telle qu'un service en réseau (par exemple, le web, une base de données, le courrier électronique). Puisque la disponibilité concerne l'accessibilité aux ressources d'information, les attaques qui consomment de la largeur de bande de réseau, des cycles du processeur ou de l'espace disque, altèrent toutes la disponibilité de la composante touchée. La liste des valeurs possibles est présentée dans le Tableau 8. La valeur de la mesure augmente avec les conséquences subies par la composante touchée.

Tableau 8 – Incidences en matière de disponibilité

Valeur de la mesure	Description
Fortes (H)	La perte de disponibilité est totale, et l'attaquant est en mesure de refuser tout accès aux ressources dans la composante touchée. Cette perte perdure (pendant que l'attaquant poursuit son attaque) ou elle persiste (même après la fin de l'attaque). A défaut, l'attaquant peut refuser certains accès, mais la perte de disponibilité a des conséquences directes et graves pour la composante touchée. Par exemple, même s'il ne peut pas interrompre les connexions existantes, l'attaquant peut empêcher l'établissement de nouvelles connexions. Il peut exploiter une vulnérabilité à plusieurs reprises, avec perte d'une petite portion de mémoire à chaque attaque réussie, ce qui rendra, après plusieurs exploitations, le service totalement indisponible.
Faibles (L)	La mise à disposition des ressources est de moins bonne qualité ou est interrompue. Même s'il peut exploiter de façon répétée une vulnérabilité, l'attaquant n'a pas la possibilité d'empêcher complètement les utilisateurs légitimes d'accéder aux services. Les ressources dans la composante touchée sont soit partiellement disponibles tout le temps, soit entièrement disponibles pendant une partie du temps seulement, mais dans l'ensemble, il n'y a pas de conséquences directes et graves pour la composante touchée.
Aucune (N)	Aucune incidence en matière de disponibilité dans la composante touchée n'est observée.

6.3 Mesures temporelles

Les mesures temporelles rendent compte de l'état des techniques d'exploitation ou de la disponibilité des codes, de la présence de correctifs ou de solutions de repli, ou de la confiance que l'on a dans la description d'une vulnérabilité.

6.3.1 Maturité du code d'exploitation (E)

Cette mesure, qui quantifie la probabilité qu'une vulnérabilité soit attaquée, est en général fondée sur l'état des techniques d'exploitation, sur la disponibilité des codes d'exploitation ou sur l'exploitation sauvage active.

La mise à disposition publique de codes d'exploitation faciles à utiliser accroît le nombre d'attaquants potentiels et permet aux non-experts d'en faire partie, ce qui ne fait qu'aggraver la vulnérabilité. Initialement, l'exploitation concrète peut n'être que théorique. Elle peut être suivie par la publication de codes types de validation, de codes fonctionnels d'exploitation ou de détails techniques suffisant à exploiter la vulnérabilité. En outre, le code d'exploitation disponible peut évoluer d'un code type de validation jusqu'à un code d'exploitation qui permet d'exploiter la vulnérabilité de manière cohérente. Lorsque la situation est grave, il peut être cheminé par le réseau sous la forme d'un ver ou d'un virus ou d'un autre outil d'attaque automatisé.

La liste des valeurs possibles est présentée dans le Tableau 9. Plus une vulnérabilité peut être exploitée facilement, plus la note de la vulnérabilité est élevée.

Tableau 9 – Maturité du code d'exploitation

Valeur de la mesure	Description
Non définie (X)	L'attribution de cette valeur à la mesure n'influencera pas la note. Il s'agit d'indiquer à l'équation d'évaluation de ne pas tenir compte de cette mesure.
Elevée (H)	Soit un code fonctionnel autonome existe, soit aucun code d'exploitation n'est requis (déclenchement manuel) et les détails sont faciles à se procurer. Le code d'exploitation fonctionne dans toutes les situations, ou il est transmis activement par un agent autonome (tel qu'un ver ou un virus). Les systèmes reliés au réseau sont susceptibles de faire l'objet de tentatives de balayage ou d'exploitation. Le niveau de développement des codes d'exploitation a atteint celui d'outils automatisés, fiables, faciles à se procurer et à employer.
Fonctionnelle (F)	Le code fonctionnel d'exploitation est disponible. Il fonctionne dans la plupart des situations où une vulnérabilité est présente.
Validation (P)	Soit un code type de validation est disponible, soit la démonstration au moyen d'une attaque est difficile pour la plupart des systèmes. Le code ou la technique ne sont pas fonctionnels dans toutes les situations et peuvent obliger l'attaquant compétent à apporter d'importantes modifications.
Non confirmée (U)	Soit aucun code d'exploitation n'est disponible, soit celui-ci est théorique.

6.3.2 Niveau de correction (RL)

Le niveau de correction d'une vulnérabilité est un facteur important pour l'établissement des priorités. Lors de sa publication initiale, une vulnérabilité type ne possède pas de correctif. Les solutions de repli et les mesures curatives peuvent être des remèdes temporaires en attendant la publication de mises à jour ou de correctifs officiels. Chacune de ces étapes respectives abaisse la note temporelle, dénotant une diminution de l'urgence à mesure que le remède devient définitif. La liste des valeurs possibles est présentée dans le Tableau 10. Moins le correctif est officiel et permanent, plus la note de la vulnérabilité est élevée.

Tableau 10 – Niveau de correction

Valeur de la mesure	Description
Non défini (X)	L'attribution de cette valeur à la mesure n'influencera pas la note. Il s'agit d'indiquer à l'équation d'évaluation de ne pas tenir compte de cette mesure.
Indisponible (U)	Soit aucune solution n'est disponible, soit il est impossible de l'appliquer.
Solution de repli (W)	Une solution non officielle, non publiée par un éditeur, est disponible. Dans certains cas, soit les utilisateurs de la technologie touchée élaboreront eux-mêmes un correctif, ou ils suivront une démarche leur permettant d'appliquer une solution de repli, ou ils réduiront la vulnérabilité d'une autre façon.
Correctif temporaire (T)	Un correctif officiel mais temporaire est disponible. C'est le cas lorsque l'éditeur publie un correctif, un outil ou une solution de repli temporaire.
Correctif officiel (O)	Une solution complète de l'éditeur est disponible. Soit l'éditeur a publié un correctif officiel, soit une mise à jour est disponible.

6.3.3 Confiance indiquée (RC)

Cette mesure quantifie le niveau de confiance, s'agissant de l'existence d'une vulnérabilité et des détails techniques connus. Parfois, seule l'existence des vulnérabilités est rendue publique, mais sans détails précis. Par exemple, des effets non souhaités peuvent être observés, mais leur origine peut être inconnue. La vulnérabilité peut être ultérieurement corroborée, pas toujours avec une certitude totale, par des recherches qui peuvent indiquer où elle se situe. Enfin, une vulnérabilité peut être confirmée par l'auteur ou l'éditeur de la technologie touchée. Lorsque l'on sait avec certitude qu'une vulnérabilité

existe, son degré d'urgence est plus élevé. Cette mesure rend également compte du niveau des connaissances techniques à la disposition des attaquants potentiels. La liste des valeurs possibles est présentée dans le Tableau 11. Plus la vulnérabilité est validée par l'éditeur ou d'autres sources recommandables, plus la note est élevée.

Tableau 11 – Confiance indiquée

Valeur de la mesure	Description
Non définie (X)	L'attribution de cette valeur à la mesure n'influencera pas la note. Il s'agit d'indiquer à l'équation d'évaluation de ne pas tenir compte de cette mesure.
Confirmée (C)	Soit des indications détaillées existent, soit une reproduction fonctionnelle est possible (les codes fonctionnels d'exploitation le permettent). Le code source est disponible pour vérifier indépendamment les affirmations des recherches, ou l'auteur ou l'éditeur du code touché a confirmé la présence de la vulnérabilité.
Raisonnable (R)	Des détails importants sont publiés, mais les chercheurs, soit n'ont pas une confiance totale en l'origine, soit n'ont pas accès au code source pour confirmer totalement l'ensemble des interactions qui peuvent avoir conduit au résultat. On peut cependant raisonnablement être confiant que le bogue est reproductible et qu'au moins une conséquence peut être vérifiée (les codes types de validation le permettent). Un exemple est le descriptif détaillé des recherches sur une vulnérabilité avec une explication (peut-être peu claire ou "laissée au lecteur à titre d'exercice") qui donne des assurances sur la manière de reproduire les résultats.
Inconnue (U)	Des indications d'effets signalent la présence d'une vulnérabilité. Soit elles révèlent que l'origine de la vulnérabilité est inconnue, soit elles diffèrent quant à l'origine ou aux incidences de la vulnérabilité. Les rapporteurs sont incertains quant à la nature véritable de la vulnérabilité, et il n'y a que peu de confiance en ce qui concerne la validité des indications ou la question de savoir si une note statique de base peut être appliquée, compte tenu des différences décrites. Un exemple est l'indication concernant un bogue, dans laquelle il est observé qu'une panne intermittente mais non reproductible a lieu, accompagnée de la corruption de la mémoire, suggérant qu'un déni de service ou éventuellement des incidences plus graves pourraient en résulter.

6.4 Mesures environnementales

Ces mesures permettent à un analyste d'adapter la note CVSS attribuée aux biens informatiques touchés, en fonction de leur importance pour l'entreprise d'un utilisateur, mesurée au moyen de contrôles de sécurité complémentaires ou alternatifs en place, qui concernent la confidentialité, l'intégrité et la disponibilité. Ces sont des équivalents modifiés des mesures de base, et les valeurs qui leur sont attribuées sont fondées sur l'emplacement de la composante dans l'infrastructure de l'entreprise.

6.4.1 Exigences de sécurité (CR, IR, AR)

Ces mesures permettent à un analyste d'adapter la note CVSS attribuée aux biens informatiques touchés, en fonction de leur importance pour l'entreprise d'un utilisateur, mesurée en termes de confidentialité, d'intégrité et de disponibilité. Cela veut dire que si un bien informatique assure une fonction commerciale pour laquelle le facteur disponibilité est le plus important, l'analyste peut attribuer à la disponibilité une valeur qui est plus grande que celles qui sont attribuées à la confidentialité ou à l'intégrité. Chacune des exigences de sécurité a trois valeurs possibles: faible, moyenne ou forte.

L'effet total sur la note environnementale est déterminé au moyen des mesures des incidences de base correspondantes modifiées. C'est à dire que ces mesures modifient la note environnementale, en pondérant les mesures modifiées des incidences en matière de confidentialité, d'intégrité ou de disponibilité. Par exemple, la mesure modifiée des incidences en matière de confidentialité (MC) a un poids plus élevé lorsque l'exigence de confidentialité (CR) est "forte". De façon analogue, ladite mesure a un poids plus faible lorsque l'exigence de confidentialité est "faible". Et pour finir, ladite mesure a un poids neutre lorsque l'exigence de confidentialité est "moyenne". La même procédure s'applique à l'intégrité et à la disponibilité.

Il convient de noter que l'exigence de confidentialité n'influencera pas la note environnementale si la valeur attribuée aux incidences (de base modifiées) en matière de confidentialité est "aucune". Par ailleurs, le renforcement de l'exigence de confidentialité de "moyenne "à "forte" ne modifiera pas la note environnementale lorsque la valeur attribuée aux incidences (de base modifiées) est "forte". Cela résulte du fait que la note partielle des incidences modifiées (partie de la note de base modifiée caractérisant les incidences) a déjà atteint la valeur maximale de 10.

La liste des valeurs possibles est présentée dans le Tableau 12. Pour simplifier, le même tableau est employé pour les trois mesures. Plus l'exigence de sécurité est forte, plus la note est élevée (il faut se souvenir que l'exigence par défaut est celle qui est moyenne).

Tableau 12 – Exigences de sécurité

Valeur de la mesure	Description
Non définies (X)	L'attribution de cette valeur à la mesure n'influencera pas la note. Il s'agit d'indiquer à l'équation de ne pas tenir compte de cette mesure.
Fortes (H)	La perte [de la confidentialité | de l'intégrité | de la disponibilité] peut avoir des effets préjudiciables catastrophiques pour l'entreprise ou les personnes qui lui sont associées (par exemple, les employés, les clients).
Moyennes (M)	La perte [de la confidentialité | de l'intégrité | de la disponibilité] peut avoir des effets préjudiciables graves pour l'entreprise ou les personnes qui lui sont associées (par exemple, les employés, les clients).
Faibles (L)	La perte [de la confidentialité | de l'intégrité | de la disponibilité] peut n'avoir que des effets préjudiciables limités pour l'entreprise ou les personnes qui lui sont associées (par exemple, les employés, les clients).

6.4.2 Mesures de base modifiées

Ces mesures permettent à un analyste d'adapter les mesures de base en fonction des modifications qui ont été apportées dans son environnement. En d'autres termes, si un environnement a conduit à des modifications en profondeur du logiciel touché, qui entraînent une exploitabilité, un champ ou des incidences modifiés, alors il peut en être rendu compte au moyen d'une note environnementale modifiée de manière appropriée.

L'effet total sur la note environnementale est déterminé au moyen des mesures de base correspondantes. Cela veut dire que ces mesures modifient la note environnementale en réattribuant des valeurs (de base), puis en appliquant les exigences de sécurité (environnementales). Par exemple, une composante vulnérable peut être configurée par défaut pour assurer un service d'écoute, moyennant des privilèges d'administrateur. La corruption de cette composante par un attaquant pourrait conduire à des incidences en matière de confidentialité, d'intégrité ou de disponibilité qui sont toutes "fortes". Mais dans l'environnement de l'analyste, le même service Internet pourrait être assuré, moyennant des privilèges réduits. Dans ce cas, la confidentialité, l'intégrité ou la disponibilité modifiées pourraient toutes être fixées à "faibles".

Pour simplifier, seuls les noms des mesures de base modifiées sont mentionnés. Chacune des mesures environnementales modifiées a la même valeur que celle de la mesure de base correspondante, à laquelle s'ajoute une valeur "non définie".

Cette mesure a pour objet de définir les techniques d'atténuation mises en place dans un environnement donné. Il est possible d'employer les mesures modifiées pour décrire des situations dans lesquelles la note de base augmente. Par exemple, une composante peut être configurée par défaut de manière qu'il faille d'importants privilèges (PR: "importants") pour accéder à une fonction particulière, alors que, dans l'environnement de l'analyste, aucun privilège n'est nécessaire (PR: "aucun"). L'analyste peut dans ce cas employer MPR: aucun, pour rendre compte de cette situation plus grave pour son environnement.

La liste des valeurs possibles est présentée dans le Tableau 13.

Tableau 13 – Mesures de base modifiées

Mesure de base modifiée	Valeurs correspondantes
Vecteur de l'attaque modifié (MAV)	Les mêmes valeurs que celles des mesures de base correspondantes (voir les mesures de base ci-dessus), ainsi que la valeur "non définie" (par défaut)
Complexité de l'attaque modifiée (MAC)	
Privilèges requis modifiés (MPR)	
Intervention de l'utilisateur modifiée (MUI)	
Champ modifié (MS)	
Confidentialité modifiée (MC)	
Intégrité modifiée (MI)	
Disponibilité modifiée (MA)	

6.5 Echelle de notation qualitative de la gravité

Dans certains cas, il est utile de disposer d'une représentation textuelle de la note de base, de la note temporelle et de la note environnementale. Toutes les notes peuvent être mises en correspondance avec les notations qualitatives définies dans le Tableau 14[3].

Tableau 14 – Echelle de notation qualitative de la gravité

Notation	Note CVSS
Aucune	0,0
Faible	0,1-3,9
Moyenne	4,0-6,9
Elevée	7,0-8,9
Très élevée	9,0-10,0

A titre d'exemple, une note de base de 4,0 correspond à une notation de la gravité dont la valeur est "moyenne". L'emploi de ces notations qualitatives de la gravité est facultative, et il n'y aucune obligation à les mentionner lors de la publication des notes CVSS. Elles sont destinées à aider les entreprises à bien évaluer leurs processus de gestion des vulnérabilités et à bien établir leur priorité.

[3] Il convient de noter que cette mise en correspondance entre les notes quantitatives et les notes qualitatives s'applique, qu'il s'agisse du groupe de mesures de base seulement, ou de l'ensemble des groupes de mesures de base, de mesures temporelles et de mesures environnementales.

6.6 Chaîne vectorielle

La chaîne vectorielle CVSS version 3.0 est une représentation textuelle d'un ensemble de mesures CVSS. Elle est couramment employée pour consigner ou transférer des informations sur les mesures CVSS sous une forme concise.

La chaîne vectorielle version 3.0 débute par l'étiquette "CVSS:" et les chiffres correspondant à la version en vigueur "3.0". Des informations sur les mesures suivent sous la forme d'un ensemble de mesures, chaque mesure étant précédée d'une barre oblique vers l'avant "/", en tant que délimiteur. Chaque mesure porte un nom de mesure sous une forme abrégée, deux-points ":" et sa valeur associée sous une forme abrégée. Les formes abrégées sont définies ci-dessus dans la présente spécification (entre parenthèses, après chaque nom de mesure et chacune des valeurs de mesure) et sont résumées dans le tableau ci-après.

Les mesures peuvent être spécifiées dans un ordre quelconque, même si le Tableau 15 les mentionne dans l'ordre qui est préféré. Toutes les mesures de base doivent faire partie d'une chaîne vectorielle. Les mesures temporelles et environnementales sont en option, et les mesures omises peuvent être considérées comme ayant la valeur "non définie" (X). Si cela est souhaité, les mesures dont la valeur est "non définie" peuvent explicitement faire partie d'une chaîne vectorielle. Les programmes de lecture des chaînes vectorielles version 3.0 doivent accepter les mesures dans un ordre quelconque et traiter les mesures temporelles et environnementales non spécifiées comme étant "non définies". Une chaîne vectorielle ne doit pas comporter plus d'une fois la même mesure.

Tableau 15 – Vecteurs de base, vecteurs temporels et vecteurs environnementaux

Groupe de mesures	Nom de la mesure et forme abrégée	Valeurs possibles	Obligatoire?
Mesures de base	Vecteur de l'attaque, AV	[N,A,L,P]	Oui
	Complexité de l'attaque, AC	[L,H]	Oui
	Privilèges requis, PR	[N,L,H]	Oui
	Intervention de l'utilisateur, UI	[N,R]	Oui
	Champ, S	[U,C]	Oui
	Confidentialité, C	[H,L,N]	Oui
	Intégrité, I	[H,L,N]	Oui
	Disponibilité, A	[H,L,N]	Oui
Mesures temporelles	Maturité du code d'exploitation, E	[X,H,F,P,U]	Non
	Niveau de correction, RL	[X,U,W,T,O]	Non
	Confiance indiquée, RC	[X,C,R,U]	Non

Tableau 15 – Vecteurs de base, vecteurs temporels et vecteurs environnementaux

Groupe de mesures	Nom de la mesure et forme abrégée	Valeurs possibles	Obligatoire?
Mesures environnementales	Confidentialité requise, CR	[X,H,M,L]	Non
	Intégrité requise, IR	[X,H,M,L]	Non
	Disponibilité requise, AR	[X,H,M,L]	Non
	Vecteur de l'attaque modifié, MAV	[X,N,A,L,P]	Non
	Complexité de l'attaque modifiée, MAC	[X,L,H]	Non
	Privilèges requis modifiés, MPR	[X,N,L,H]	Non
	Intervention de l'utilisateur modifiée, MUI	[X,N,R]	Non
	Champ modifié, MS	[X,U,C]	Non
	Confidentialité modifiée, MC	[X,N,L,H]	Non
	Intégrité modifiée, MI	[X,N,L,H]	Non
	Disponibilité modifiée, MA	[X,N,L,H]	Non

Par exemple, une vulnérabilité avec des valeurs des mesures de base de "vecteur de l'attaque: réseau, complexité de l'attaque: faible, privilèges requis: importants, intervention de l'utilisateur: aucune, champ: non modifié, incidences en matière de confidentialité: faibles, incidences en matière d'intégrité: faibles, incidences en matière de disponibilité: aucune", sans spécification de mesures temporelles ou environnementales, produirait le vecteur suivant:

– CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

Le même exemple auquel il est ajouté "exploitabilité: fonctionnelle, niveau de correction: non défini", les mesures étant présentées dans un ordre qui n'est pas celui qui est préféré, produirait le vecteur suivant:

– CVSS:3.0/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

6.7 Définition du schéma XML CVSS version 3.0

La définition du schéma XML (XSD) CVSS, qui établit la structure du fichier XML contenant les valeurs des mesures XML, est utile à ceux qui souhaitent consigner ou transférer ces données au format XML. La définition est disponible à l'adresse suivante: https://www.first.org/cvss/cvss-v3.0.xsd.

6.8 Equations CVSS version 3.0

Les équations CVSS version 3.0 sont définies ci-après.

6.8.1 Note de base

La note de base est fonction de l'équation de la note partielle des incidences et de l'équation de la note partielle de l'exploitabilité. La note de base est définie comme suit:

If (Impact sub score <= 0) 0 else,

Scope Unchanged [4] $Roundup(Minimum[(Impact + Exploitability), 10])$

Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

et la note partielle des incidences (ISC) est définie comme suit:

Scope Unchanged $6.42 \times ISC_{Base}$

Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

où

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) \times \left(1 - Impact_{Integ}\right) \times \left(1 - Impact_{Avail}\right)\right]$$

La note partielle de l'exploitabilité est définie comme suit:

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

6.8.2 Note temporelle

La note temporelle est définie comme suit:

$$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$$

6.8.3 Note environnementale

La note environnementale est définie comme suit:

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged
Round up(Round up (Minimum [
× (M.Impact + M.Exploitability) ,10])
× Exploit Code Maturity
× Remediation Level
× Report Confidence)

If Modified Scope is Changed
Round up(Round up (Minimum [1.08
× (M.Impact + M.Exploitability) ,10])
× Exploit Code Maturity
× Remediation Level
× Report Confidence)

Et la note partielle des incidences modifiées est définie comme suit:

If Modified Scope is Unchanged $6.42 \times \left[ISC_{Modified}\right]$

If Modified Scope is Changed $7.52 \times \left[ISC_{Modified} - 0.029\right]$-$3.25 \times \left[ISC_{Modified} - 0.02\right]^{15}$

4 Par "Round up" (arrondi), on entend le plus petit nombre, à une décimale, qui est égal ou supérieur à la valeur initiale. L'arrondi de (4,02) est 4,1 et celui de (4,00) est 4,0.

où:

$$ISC_{Modified} = Minimum\left[\left[1 - \left(1 - M.I_{Conf} \times CR\right) \times \left(1 - M.I_{Integ} \times IR\right) \times \left(1 - M.I_{Avail} \times AR\right)\right], 0.915\right]$$

La note partielle de l'exploitabilité modifiée est définie comme suit:

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$$

6.8.4 Niveaux des mesures

Les valeurs des mesures sont définies dans le Tableau 16.

Tableau 16 – Valeurs des mesures

Mesure	Valeur de la mesure	Valeur numérique
Vecteur de l'attaque/ vecteur de l'attaque modifié	Réseau	0,85
	Réseau adjacent	0,62
	Accès local	0,55
	Accès physique	0,2
Complexité de l'attaque/ complexité de l'attaque modifiée	Faible	0,77
	Grande	0,44
Privilèges requis/ privilèges requis modifiés	Aucun	0,85
	Faibles	0,62 (0,68 si le champ/ champ modifié est changé)
	Grands	0,27 (0,50 si le champ/ champ modifié est changé)
Intervention de l'utilisateur/ intervention de l'utilisateur modifiée	Aucune	0,85
	Requise	0,62
Incidences C, I, A/ incidences C, I, A modifiées	Fortes	0,56
	Faibles	0,22
	Aucune	0
Maturité du code d'exploitation	Non définie	1
	Elevée	1
	Fonctionnelle	0,97
	Validation	0,94
	Non confirmée	0,91
Niveau de correction	Non défini	1
	Indisponible	1
	Solution de repli	0,97
	Correctif temporaire	0,96
	Correctif officiel	0,95

Tableau 16 – Valeurs des mesures

Mesure	Valeur de la mesure	Valeur numérique
Confiance indiquée	Non définie	1
	Confirmée	1
	Raisonnable	0,96
	Inconnue	0,92
Exigences de sécurité – Exigences de C, I, A (CR)	Non définies	1
	Fortes	1,5
	Moyennes	1
	Faibles	0,5

6.8.5 Concernant les équations et l'évaluation du système CVSS version 3.0

La formulation CVSS version 3.0 permet d'obtenir une approximation mathématique de toutes les combinaisons de mesures possibles, classées par ordre de gravité (sous la forme d'un tableau de recherche des vulnérabilités). Afin d'aboutir à l'élaboration de cette formulation CVSS version 3.0, le Groupe d'intérêt (SIG) a établi un tableau de recherche en attribuant des valeurs de mesure version 3.0 aux vulnérabilités réelles, et un degré de gravité (faible, moyen, élevé ou très élevé). Après avoir défini des intervalles numériques acceptables pour chaque degré de gravité, le Groupe a ensuite collaboré avec Deloitte & Touche LLP pour ajuster les paramètres de la formulation afin d'aligner les combinaisons de mesures version 3.0 sur les degrés de gravité qu'il avait proposés.

Etant donné que le nombre de notes chiffrées est limité (101 notes, comprises entre 0,0 et 10,0), des combinaisons de mesures multiples peuvent produire la même note chiffrée. Par ailleurs, certaines notes chiffrées peuvent être omises parce que les poids et les calculs sont déduits du degré de gravité des combinaisons de mesures. En outre, dans certains cas, les combinaisons de mesures peuvent s'écarter du seuil de gravité souhaité. Cela est inévitable et une correction simple n'est pas facile à effectuer, parce que l'ajustement d'une valeur de la mesure ou d'un paramètre d'une équation pour corriger l'écart peut causer d'autres écarts, potentiellement plus graves.

Par consensus, comme cela avait été fait pour le système CVSS version 2.0, il a été accepté une valeur de 0,5 pour l'écart. Cela veut dire que toutes les combinaisons des valeurs de mesure employées pour les poids et les calculs, permettront d'obtenir une note chiffrée dont le degré de gravité appartient à l'intervalle qui lui a été attribué, ou s'écarte de 0,5 de cet intervalle. Par exemple, une combinaison qui est susceptible d'avoir une note "élevée" peut avoir une note chiffrée comprise entre 6,6 et 9,3. Finalement, afin d'assurer la rétrocompatibilité, le système CVSS version 3.0 a conservé le domaine de valeurs compris entre 0,0 et 10,0.

Appendice I

Manuel d'utilisation du système CVSS version 3.0

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

I.1 Introduction

Le présent manuel complète le document officiel qui contient la spécification du système CVSS version 3.0, en donnant des informations supplémentaires et en mettant en évidence les modifications pertinentes apportées à la version 2.0, ainsi qu'en donnant des orientations en matière d'évaluation et en proposant une rubrique sur l'évaluation.

Le système d'évaluation des vulnérabilités courantes (CVSS) est un moyen qui permet de déterminer les principales caractéristiques d'une vulnérabilité, d'obtenir une note chiffrée rendant compte de sa gravité, et de donner une représentation textuelle de cette note. La note chiffrée peut être traduite sur le plan qualitatif (degré de gravité faible, moyen, élevé ou très élevé) afin d'aider les entreprises à bien évaluer leurs processus de gestion des vulnérabilités et à bien établir leur priorité.

Le système CVSS a trois grands avantages:

- Il permet d'obtenir des notes normalisées des vulnérabilités. Lorsqu'une entreprise emploie un seul algorithme pour l'évaluation des vulnérabilités sur l'ensemble de ses plates-formes informatiques, elle peut s'appuyer sur une seule politique de gestion des vulnérabilités pour définir le temps maximal nécessaire à la confirmation et à la correction de la vulnérabilité donnée.
- Il définit un cadre ouvert. Les utilisateurs peuvent être désorientés lorsqu' une note arbitraire est attribuée à une vulnérabilité par une entité tierce. Avec le système CVSS, les différentes caractéristiques employées pour obtenir une note sont transparentes.
- Le système CVSS permet d'attribuer un degré de priorité. Lorsque la note environnementale est calculée, la vulnérabilité est considérée dans le contexte propre à chaque entreprise, et cette note aide à mieux comprendre le risque que présente ladite vulnérabilité pour l'entreprise.

Depuis sa publication initiale en 2004, le système CVSS a été adopté à grande échelle. En septembre 2007, le système CVSS version 2.0 a été adopté dans le cadre de la norme Payment Card Industry Data Security Standard (PCI DSS). Afin de se conformer à cette norme, les commerçants employant les cartes de crédit doivent prouver qu'aucun de leurs systèmes informatiques ne présente une vulnérabilité dont la note CVSS est supérieure ou égale à 4. En 2007, le National Institute of Standards and Technology (NIST) a intégré le système CVSS version 2.0 dans son protocole Security Content Automation Protocol (SCAP)[5]. En avril 2011, le système CVSS version 2.0 a été officiellement adopté en tant que norme internationale d'évaluation des vulnérabilités (UIT-T X.1521)[6].

I.2 Modifications apportées au système CVSS version 3.0

Etant donné l'adoption à grande échelle du système CVSS version 2.0, un certain nombre de possibilités d'amélioration ont été recensées, qui ont conduit à l'élaboration de la version 3.0. Ces améliorations sont décrites en détail ci-après.

5 Voir http://scap.nist.gov/.

6 Voir http://www.itu.int/rec/T-REC-X.1521-201104-I/fr.

I.2.1 Champ, composante vulnérable et composante touchée

Le système CVSS version 2.0 présentait des difficultés aux éditeurs lorsqu'ils souhaitaient évaluer les vulnérabilités qui compromettaient entièrement leurs logiciels, mais n'avaient que des incidences partielles sur le système d'exploitation central. Dans la version 2.0, les vulnérabilités sont notées par rapport au système d'exploitation central, ce qui a conduit un éditeur d'applications à adopter la convention métrique "partial+" pour les incidences[7]. Cette question est traitée dans le système CVSS version 3.0 au moyen de mises à jour, permettant de préciser l'endroit où les mesures des incidences sont notées, et de l'introduction d'une nouvelle mesure nommée "champ" (examinée plus en détail ci-après). Cela a conduit à une modification conceptuelle importante dans le système CVSS version 3.0, donnant la possibilité de noter les vulnérabilités, qui existent dans une composante logicielle (que nous nommons de façon formelle la *composante vulnérable*), mais ont des incidences sur d'autres composantes logicielles ou matérielles ou sur les composantes de réseau distinctes (que nous nommons de façon formelle la *composante touchée*), comme illustré dans la Figure I.1[8].

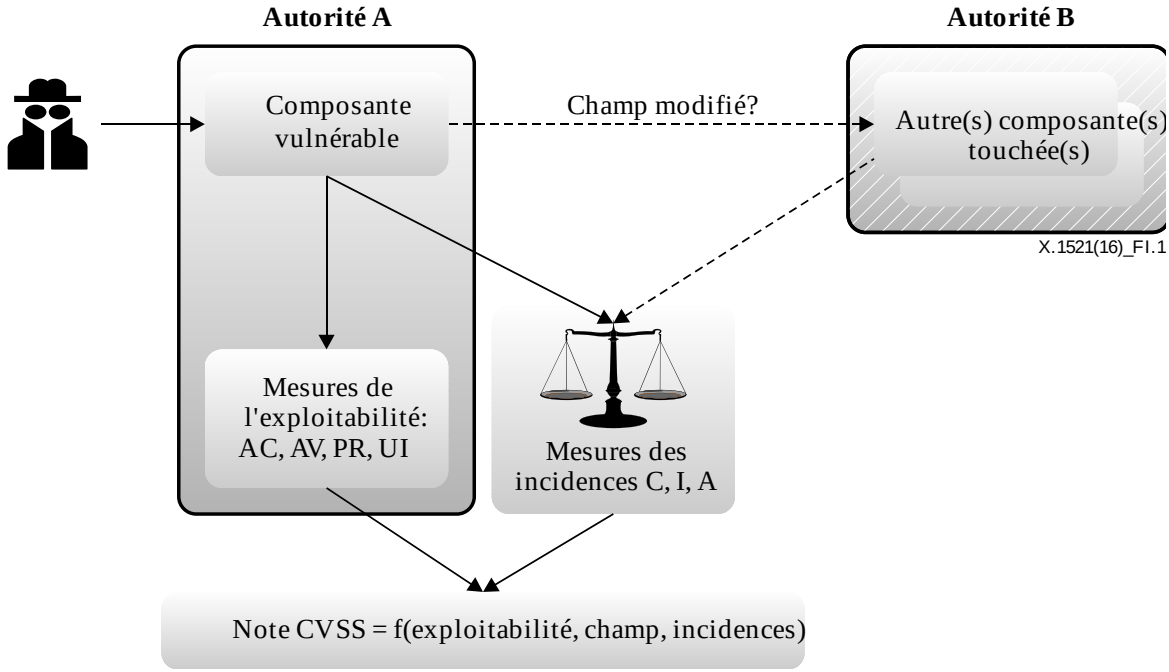


Figure I.1 – Modification de champ

Considérons par exemple une vulnérabilité dans une machine virtuelle qui compromet le système d'exploitation central. La composante vulnérable est la machine virtuelle, tandis que la composante touchée est le système d'exploitation central. Comme ces deux composantes gèrent de façon indépendante leurs privilèges d'accès aux ressources informatiques, elles relèvent, pour ce qui est des autorisations, d'autorités différentes. Dans la Figure I.1, la machine virtuelle est gérée par l'"autorité A", tandis que le système d'exploitation central est géré par l'"autorité B". Lorsque deux autorités sont impliquées dans l'exploitation d'une vulnérabilité, le système CVSS considère qu'une *modification de champ* s'est produite. Il est rendu compte de cette situation au moyen de la nouvelle mesure "champ".

---

7 Par exemple, voir http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html.

8 Il convient de noter que, tandis que la composante vulnérable est un programme logiciel (système d'exploitation central, application Internet, pilote de dispositif, etc.), la composante touchée peut être soit un autre programme logiciel, soit un dispositif matériel, soit une ressource de réseau.

Comme illustré dans la Figure I.1, lors de l'évaluation des vulnérabilités dans le système CVSS version 3.0, les mesures de l'exploitabilité sont notées par rapport à la composante vulnérable. A savoir, elles sont notées après examen de la composante qui présente une faille de codage. D'autre part, les mesures des incidences sont notées par rapport à la composante touchée. Parfois, la composante vulnérable peut être la même que la composante touchée, auquel cas aucune modification de champ ne s'est produite. Mais dans d'autres cas, il peut y avoir des incidences sur la composante vulnérable et sur la composante touchée. Une modification de champ s'est alors produite, et les mesures des incidences en matière de confidentialité, d'intégrité et de disponibilité devraient rendre compte des incidences soit sur la composante vulnérable, soit sur la composante touchée, la composante ayant subi les incidences les plus graves étant retenue.

Dans le cas d'une vulnérabilité qui permet le vol d'un fichier de mots de passe, l'attaquant peut éventuellement entreprendre des démarches pour accéder de manière non autorisée à un compte, mais la conséquence la plus directe est une perte de confidentialité du fichier système local. Dans ce cas, il n'y a pas de modification de champ. Mais, dans le cas d'une vulnérabilité qui permet le remplacement d'un tableau ARP du routeur par l'attaquant, les incidences sont doubles. D'abord sur le fichier système du routeur (incidences en matière d'intégrité de la composante vulnérable), puis sur les services Internet desservis par le routeur (incidences en matière de disponibilité des systèmes touchés). Parce que la note doit rendre compte des conséquences les plus graves, la mesure des incidences peut faire état soit de la perte d'intégrité de la composante vulnérable, soit de la perte de disponibilité des services Internet, la composante ayant subi les incidences les plus graves étant retenue[9].

I.2.2 Vecteur de l'attaque

Le "vecteur d'accès" (de la version 2.0) a été renommé "vecteur de l'attaque", mais il rend toujours compte de la "distance" de l'attaquant par rapport à la composante vulnérable. A savoir, la note de base sera d'autant plus grande que l'attaquant est loin de la composante vulnérable (en termes de distance dans les réseaux logique et physique). En outre, cette mesure distingue les attaques locales qui nécessitent un accès local au système (tel que lors de l'attaque d'une application d'ordinateur de bureau) des attaques physiques qui nécessitent un accès physique à la plate-forme pour exploiter la vulnérabilité (tel que lors de l'attaque par l'intermédiaire d'un bus Firewire, d'un bus USB ou d'un bélier).

I.2.3 Complexité de l'attaque

La "complexité de l'accès" (de la version 2.0) confondait deux questions: la situation logicielle, matérielle ou au niveau du réseau, échappant au contrôle de l'attaquant, qui doit exister pour pouvoir exploiter une vulnérabilité avec succès (par exemple, une situation de course logicielle ou la configuration d'une application), et la nécessité d'une intervention de l'homme (par exemple, la nécessité qu'un utilisateur exécute un code exécutable malveillant). La complexité de l'accès a donc été scindée en deux, la mesure "complexité de l'attaque" (qui concerne la première situation) et la mesure "**intervention de l'utilisateur**" (qui concerne la deuxième situation).

I.2.4 Privilèges requis

Cette nouvelle mesure "**privilèges requis**" remplace la mesure "authentification" de la version 2.0. Au lieu de mesurer le *nombre de fois* où un attaquant doit s'authentifier dans un système, la mesure "privilèges requis" rend compte du *niveau d'accès* requis pour réussir une attaque. Les valeurs de la mesure, en particulier, "grands", faibles" et "aucun", rendent compte des privilèges requis par l'attaquant pour exploiter la vulnérabilité.

---

9 Pour plus d'informations, voir le document intitulé Exemples qui accompagne le présent manuel.

I.2.5 Mesures des incidences

Les valeurs des mesures des "**incidences en matière de confidentialité, d'intégrité et de disponibilité**" de la version 2.0 qui étaient "aucune", "partielles" et "complètes" ont été remplacées par "aucune", "faibles" et "fortes". Plutôt que de correspondre au *pourcentage* global (la proportion) des systèmes touchés par une attaque, les nouvelles valeurs des mesures rendent compte de l'*importance* globale des incidences d'une attaque. Par exemple, alors que la vulnérabilité au bogue "saignement du coeur" (*heartbleed*)[10] entraîne seulement la perte d'un petit nombre d'informations, les incidences sont plutôt graves. Dans le système CVSS version 2.0, ces incidences auraient reçu la note "partielles", tandis que, dans le système CVSS version 3.0, elles reçoivent la note "fortes", qui convient mieux.

En outre, dans l'exemple ci-dessus, les mesures des incidences sont maintenant à l'image de la conséquence pour la composante touchée. Et la composante touchée peut être la même ou pas que la composante qui présente la vulnérabilité exploitée, ou en différer

I.2.6 Mesures temporelles

L'importance des mesures temporelles a été diminuée dans la version 3.0 par rapport à la version 2.0. La mesure "exploitabilité" a été renommée "maturité du code d'exploitation" afin de mieux correspondre à ce que la mesure évalue.

I.2.7 Mesures environnementales

Les mesures environnementales "distribution des cibles" et "dommages collatéraux potentiels" ont été remplacées par des mesures de base "modifiées" qui intègrent les contrôles de l'atténuation ou les failles de contrôle qui pourraient être présents dans l'environnement de l'utilisateur et pourraient réduire ou augmenter les incidences d'une vulnérabilité exploitée avec succès.

I.2.8 Echelle de notation qualitative

Certaines entreprises ont mis au point des systèmes permettant de mettre en correspondance les notes de base du système CVSS version 2.0 avec des notations qualitatives. Le système CVSS version 3.0 contient une mise en correspondance normalisée entre les notes chiffrées et les notations de la gravité "aucune", "faible", "moyenne", "élevée" et "très élevée", comme expliqué dans le document de spécification du système CVSS version 3.0. L'emploi de ces notations qualitatives de la gravité est facultatif, et il n'y a aucune obligation à les mentionner lors de publication des notes CVSS.

Les entreprises employant les notes CVSS version 3.0 qui souhaitent utiliser un *autre* système de notation de la gravité sont priées pour éviter toute confusion d'utiliser des termes différents pour les notations ou d'indiquer clairement que leurs notations ne concordent pas avec la spécification du système CVSS version 3.0.

I.2.9 Synthèse des modifications

Une conséquence importante de ces modifications est que les notes de la version 2.0 et celles de la version 3.0 peuvent ne pas toujours être comparables. Par exemple, une application vulnérable au point d'être entièrement compromise, s'agissant des incidences en matière de confidentialité, d'intégrité et de disponibilité, serait notée dans la version 2.0 au moyen de la valeur de la mesure "partielles". Dans la version 3.0, par contre, cette même vulnérabilité, s'agissant toujours des incidences en matière de confidentialité, d'intégrité et de disponibilité, serait maintenant notée au moyen de la valeur de la mesure "fortes".

Une synthèse des modifications apportées à la version 2.0 est présentée dans le Tableau I.1.

---

10 Voir http://heartbleed.com/.

Tableau I.1 – Modifications apportées lors du passage du système CVSS version 2.0 au système CVSS version 3.0

Version 2.0	Version 3.0
Les vulnérabilités sont notées par rapport aux incidences globales sur la plate-forme centrale.	Les vulnérabilités sont maintenant notées par rapport aux incidences sur la composante touchée.
Il n'est pas tenu compte des situations dans lesquelles une vulnérabilité dans une application touche d'autres applications du même système.	Une nouvelle mesure "champ" concerne maintenant les vulnérabilités qui sont telles que l'*objet touché* (la composante touchée) est différent de l'*objet vulnérable* (la composante vulnérable).
Le vecteur d'accès peut confondre les attaques qui nécessitent un accès local au système et les attaques physiques du matériel.	Il est maintenant distingué, dans la mesure "vecteur de l'attaque", entre les valeurs "locales" et les valeurs "physiques".
Dans certains cas, la "complexité de l'accès" confondait la configuration du système et l'intervention de l'utilisateur.	Cette mesure est scindée en la mesure "complexité de l'attaque" (rendant compte de la complexité du système) et la mesure "intervention de l'utilisateur" (rendant compte de la participation de l'utilisateur à la réussite d'une attaque).
Dans la pratique, les notes des mesures "authentification" ne rendaient compte que de deux types de conséquences parmi les trois types possibles, et ne rendaient pas bien compte de l'aspect visé d'une vulnérabilité.	Remplaçant la mesure "authentification", une nouvelle mesure "privilèges requis" rend maintenant compte des privilèges les plus importants requis par l'attaquant, plutôt que du nombre de fois où celui-ci doit s'authentifier.
Les mesures des "incidences" rendaient compte du taux des incidences sur une application vulnérable.	Les valeurs des mesures des "incidences" rendent maintenant compte de l'importance des incidences et sont renommées "fortes", "faibles" et "aucune".
Les mesures environnementales "distribution des cibles" et "dommages collatéraux potentiels" ne se sont pas révélées utiles.	Les mesures "distribution des cibles" et "dommages collatéraux potentiels" ont été remplacées par des mesures intégrant les facteurs d'atténuation.
Le système CVSS version 2.0 ne pouvait pas prendre en charge l'évaluation des vulnérabilités multiples, visées au cours d'une même attaque.	Bien que n'étant pas une mesure au sens formel, des orientations sur l'évaluation des vulnérabilités multiples sont données dans le paragraphe intitulé "enchaînement des vulnérabilités".
Aucune ligne directrice officielle de notation qualitative n'était fournie.	Des intervalles numériques sont mis en correspondance avec une échelle de notation qualitative à 5 points.

I.3 Orientations en matière d'évaluation

Ci-après sont données aux analystes un certain nombre de suggestions à considérer lors de l'évaluation des vulnérabilités à l'aide du système CVSS version 3.0.

I.3.1 Evaluation CVSS dans le cycle de vie de l'exploitation d'une vulnérabilité

Pour déterminer à quelle étape il faut noter les incidences des vulnérabilités, les analystes doivent restreindre celles-ci et ne considérer que les conséquences raisonnables auxquelles une attaque peut conduire avec certitude. La note partielle de l'exploitabilité devrait au moins rendre compte de la possibilité qu'il y ait des incidences, mais des détails décrivant la vulnérabilité peuvent aussi être pris en compte. Considérons, par exemple, les deux vulnérabilités suivantes:

Dans le cas de la vulnérabilité 1, un attaquant non authentifié peut envoyer une demande banale spécialement conçue à un serveur web, qui amène celui-ci à divulguer en clair le mot de passe du compte du serveur principal (de l'administrateur). A partir de la note partielle de l'"exploitabilité" et de la description de la vulnérabilité, l'analyste peut seulement déduire que l'attaquant dispose d'un accès lui permettant d'envoyer une demande spécialement conçue au serveur web afin d'exploiter la vulnérabilité. Les incidences devraient en rester là. Alors que l'attaquant *peut* être en mesure d'employer ces pouvoirs pour exécuter ultérieurement un code en tant qu'administrateur, on ne sait pas si l'attaquant dispose de l'accès à une invite de connexion ou d'une méthode, fondée sur ces pouvoirs, qui lui permette d'exécuter des commandes. L'accès à ce mot de passe constitue seulement une perte directe et grave de "confidentialité":

– Note de base: 7.5 [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N].

Dans le cas de la vulnérabilité 2, un utilisateur local disposant de privilèges limités peut envoyer une demande banale spécialement conçue au système d'exploitation, qui amène celui-ci à divulguer en clair le mot de passe du compte du serveur principal (de l'administrateur). A partir de la note partielle de l'"exploitabilité" et de la description de la vulnérabilité, l'analyste peut déduire que l'attaquant dispose d'un accès au système d'exploitation et peut se connecter en tant qu'attaquant local avec des privilèges limités. L'accès à ce mot de passe constitue une perte grave de "confidentialité", d'"intégrité" et de "disponibilité", parce que l'attaquant peut émettre des commandes comme si elles émanaient du compte du serveur principal ou de l'administrateur (en supposant que l'attaquant a pu se déconnecter de son propre compte et se reconnecter en tant que serveur principal):

– Note de base: 7.8 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H].

I.3.2 Incidences en matière de confidentialité et d'intégrité comparées aux incidences en matière de disponibilité

La mesure des incidences en matière de confidentialité et d'intégrité concerne les incidences sur les *données* utilisées par le service, par exemple, un contenu web altéré dans un but malveillant ou des fichiers système qui ont été volés. La mesure des incidences en matière de disponibilité concerne l'*exploitation* du service. Elle renvoie à la qualité de fonctionnement et à l'exploitation du service lui-même, et non à la disponibilité des données. Considérons une vulnérabilité dans un service Internet tel que le web, le courrier électronique ou le système de noms de domaine (DNS), qui permet à un attaquant de modifier ou de supprimer tous les fichiers dans un répertoire. Cela n'aurait d'incidences qu'en matière d'"intégrité", plutôt qu'en matière de "disponibilité". La raison en est que le service web fonctionne toujours convenablement, mais il renvoie des contenus altérés.

I.3.3 Vulnérabilités locales exploitées par des attaquants distants

Dans le système CVSS version 2.0, le conseil de notation N° 5 énonce: "Lorsqu'une vulnérabilité peut être exploitée localement et à partir du réseau, il faut choisir la valeur "réseau". Quand une vulnérabilité peut être exploitée localement et à partir de réseaux adjacents mais pas à partir de réseaux distants, la valeur "réseau adjacent" doit être choisie. Lorsqu'une vulnérabilité peut être exploitée à partir du réseau adjacent et de réseaux distants, il faut choisir la valeur "réseau"". Cette position a parfois prêté à confusion dans les cas où, en exploitant une vulnérabilité au niveau de l'analyse des fichiers, un attaquant incite un utilisateur à télécharger un document mal formé à partir d'un serveur web distant. Dans un tel cas, les analystes employant le système CVSS version 2.0 attribueraient à ces vulnérabilités la valeur "réseau", les notes formant les chaînes de mesures AV:N/AC:M/Au:N/C:P/I:P/A:P ou AV:N/AC:M/Au:N/C:C/I:C/A:C.

Ce conseil a été amélioré dans le système CVSS version 3.0 en clarifiant les définitions des valeurs "réseau" et "réseau adjacent" de la mesure "vecteur de l'attaque". Plus précisément, les analystes ne devraient noter que les vulnérabilités "réseau" et "réseau adjacent", lorsqu'elles sont liées à la pile du réseau. Les vulnérabilités qui nécessitent l'intervention de l'utilisateur pour télécharger ou recevoir des contenus malveillants (qui pourraient aussi être fournis localement, au moyen de pilotes USB par exemple) devraient être notées comme étant "locales".

Par exemple, une vulnérabilité au niveau de l'analyse des documents, qui n'a pas besoin du réseau pour être exploitée, devrait en général être notée au moyen de la valeur "locale", quelle que soit la méthode employée pour diffuser un tel document malveillant (il pourrait par exemple s'agir d'un lien vers un site web ou d'une clé USB).

I.3.4 Vulnérabilités résultant de l'exécution d'un script intersites

Dans le système CVSS version 2.0, des orientations précises étaient nécessaires pour attribuer une note différente de zéro aux vulnérabilités résultant de l'exécution d'un script intersites (XSS), parce que ces vulnérabilités étaient évaluées par rapport au système d'exploitation central qui contenait la vulnérabilité. Une vulnérabilité XSS type conduisait à une note qui décrivait des incidences partielles en matière d'intégrité, dues à la modification de la réponse du serveur web à l'utilisateur: AV:N/AC:M/Au:N/C:N/I:P/A:N. La situation était la même pour des vulnérabilités résultant de l'exécution, fondée sur un modèle objet de documents (DOM), d'un script intersites (XSS). En effet, si ces vulnérabilités peuvent être provoquées par une intervention du serveur, elles sont entièrement exploitées côté utilisateur (par exemple, lorsque le code en JavaScript envoyé par le serveur analyse la chaîne de demande envoyée au serveur).

Ceci est l'un des principaux scénarios qui ont conduit à la conception de la mesure "champ", dans lesquels les incidences touchent non pas la composante vulnérable (par exemple, le serveur web ou le code en JavaScript envoyé par le serveur), mais une composante dont les privilèges sont administrés par une autorité distincte (par exemple, l'environnement du navigateur de l'utilisateur). En raison de cela, dans le système CVSS version 3.0, les vulnérabilités résultant de l'exécution d'un script intersites ne doivent pas se restreindre aux incidences limitées ou non existantes sur le serveur, mais peuvent maintenant être notées lorsqu'il y a des incidences sur l'utilisateur. Une vulnérabilité XSS observée, qui a permis à un attaquant de fournir un lien malveillant à une victime et d'exécuter un code en JavaScript dans son navigateur, pourrait être notée comme suit:

– CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

I.3.5 Intercepteur

Le système CVSS version 3.0 prévoit maintenant explicitement l'évaluation des attaques par intercepteur. Alors qu'il n'était pas explicitement abordé dans la version 2.0, dans la version 3.0 ce type d'attaque est traité dans le cadre de la mesure "complexité de l'attaque".

I.3.6 Vulnérabilités matérielles

En outre, alors que le système CVSS est conçu en premier lieu pour évaluer les vulnérabilités et les incidences sur les logiciels, la version 3.0 est mieux adaptée à l'évaluation des incidences sur les composantes matérielles et des effets sur les réseaux.

I.3.7 Enchaînement de vulnérabilités

Le système CVSS est conçu pour classer et noter les différentes vulnérabilités. Toutefois, il est important de prendre en charge les besoins de la communauté des analystes des vulnérabilités en tenant compte des situations dans lesquelles plusieurs vulnérabilités sont exploitées au cours d'une même attaque qui vise à compromettre un ordinateur central ou une application. L'évaluation de ces vulnérabilités multiples se nomme évaluation d'un enchaînement de vulnérabilités. Il convient de

noter que ceci n'est pas une mesure au sens formel, mais que ce sujet est abordé afin que les analystes disposent d'orientations leur permettant d'évaluer ce genre d'attaque.

Lors de l'évaluation d'une chaîne de vulnérabilités, il incombe à l'analyste d'identifier les vulnérabilités qui sont regroupées, afin de pouvoir attribuer une note à la chaîne. Il faudrait qu'il établisse une liste des différentes vulnérabilités accompagnées de leurs notes, et indique la note de la chaîne. Il peut, par exemple, en faire part dans une note d'information sur les vulnérabilités, placée sur une page web.

En outre, l'analyste peut inclure d'autres types de vulnérabilités associées qui pourraient s'enchaîner avec les vulnérabilités évaluées. En particulier, il peut établir la liste des types (ou classes) génériques de vulnérabilités associées qui s'enchaînent souvent, ou décrire de manière plus détaillées les conditions préalables qui doivent exister. Par exemple, il pourrait décrire comment certaines vulnérabilités résultant de l'injection d'un code en langage de requête structuré (SQL) ouvrent la porte à une attaque au moyen de l'exécution d'un script intersites (XSS), ou comment un type particulier de débordement de la mémoire tampon peut permettre d'acquérir des privilèges locaux. L'énumération des types ou des classes génériques de vulnérabilités permet de fournir un minimum d'informations, destinées à mettre en garde les autres utilisateurs, sans risque d'informer les attaquants sur de nouvelles possibilités d'exploitation.

A défaut, l'analyste peut établir (sous la forme d'une liste des vulnérabilités, lisible et analysable en machine, en employant les identificateurs (ID) des vulnérabilités et expositions courantes (CVE) ou la liste des failles courantes (CWE)) une liste complète des vulnérabilités spécifiques associées dont il sait qu'elles s'enchaînent (ou sont susceptibles de s'enchaîner) à l'une ou à plusieurs des vulnérabilités enchaînées qui sont notées en vue de l'exploitation du système informatique. Dans le cas où une vulnérabilité ne peut être exploitée que lorsque des conditions préalables sont satisfaites (telles que l'exploitation en premier d'une autre vulnérabilité), il est possible de regrouper deux ou plusieurs notes CVSS pour décrire la chaîne des vulnérabilités en évaluant la note partielle de l'exploitabilité la moins restrictive et la note partielle des incidences les plus fortes. L'exemple suivant emploie les notes partielles de l'exploitabilité, du champ et des incidences pour décrire la chaîne:

La vulnérabilité A est représentée par le vecteur: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, et, comme celui-ci l'indique, elle ne requiert en vue de son exploitation qu'un utilisateur local avec des privilèges limités. La vulnérabilité B est représentée par le vecteur: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L, et elle donne à l'attaquant distant et sans privilège la possibilité d'exécuter un code dans un système, dont les incidences sont "faibles" si c'est un utilisateur local qui intervient en fin d'attaque. En conséquence, étant donné les chaînes A et B, la chaîne C peut être décrite comme étant la chaîne qui assure le passage des vulnérabilités B -> A: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H, et regroupe l'"exploitabilité" de la vulnérabilité B et les "incidences" de la vulnérabilité A, le champ étant inchangé dans les deux cas. En effet, si l'on peut exploiter la vulnérabilité B et en tirer, en tant qu'utilisateur local, un code d'exploitation, alors les conditions préalables qui permettent ensuite de lancer une attaque ayant des incidences en raison de la vulnérabilité A sont satisfaites.

I.4 Glossaire

Autorité: Un conteneur informatique qui accorde et administre les privilèges d'accès aux ressources. Des exemples d'autorités sont notamment une application base de données, un système d'exploitation ou un environnement de "bac à sable".

Note de la chaîne: La note de base obtenue lors de l'évaluation de deux ou de plusieurs vulnérabilités enchaînées.

Chaîne de vulnérabilités: Voir "enchaînement des vulnérabilités".

Composante: Se réfère soit à une composante logicielle, soit à une composante matérielle.

Composante logicielle: Un programme ou un module logiciel qui contient des instructions machine à exécuter, par exemple un système d'exploitation, une application Internet ou un pilote de dispositif.

Composante matérielle: Un dispositif informatique physique.

Composante touchée: La ou les composantes qui subissent les conséquences de l'exploitation de la vulnérabilité. Elles peuvent être les mêmes que les composantes vulnérables ou, si une modification de champ s'est produite, être différentes.

Privilèges: Un ensemble de droits (généralement les capacités lire/écrire/exécuter) accordés à un utilisateur ou à un processus d'utilisateur, qui définit l'accès aux ressources informatiques.

Ressources: Un logiciel ou un objet réseau auquel il est accédé, qui est modifié ou consommé par un dispositif informatique, par exemple un fichier informatique, la mémoire, les cycles CPU ou la largeur de bande du réseau.

Champ: L'ensemble des privilèges, qui sont définis et administrés par une autorité chargée des autorisations lorsque celle-ci octroie les accès aux ressources informatiques.

Vulnérabilité: Une faille dans une composante logicielle (ou matérielle).

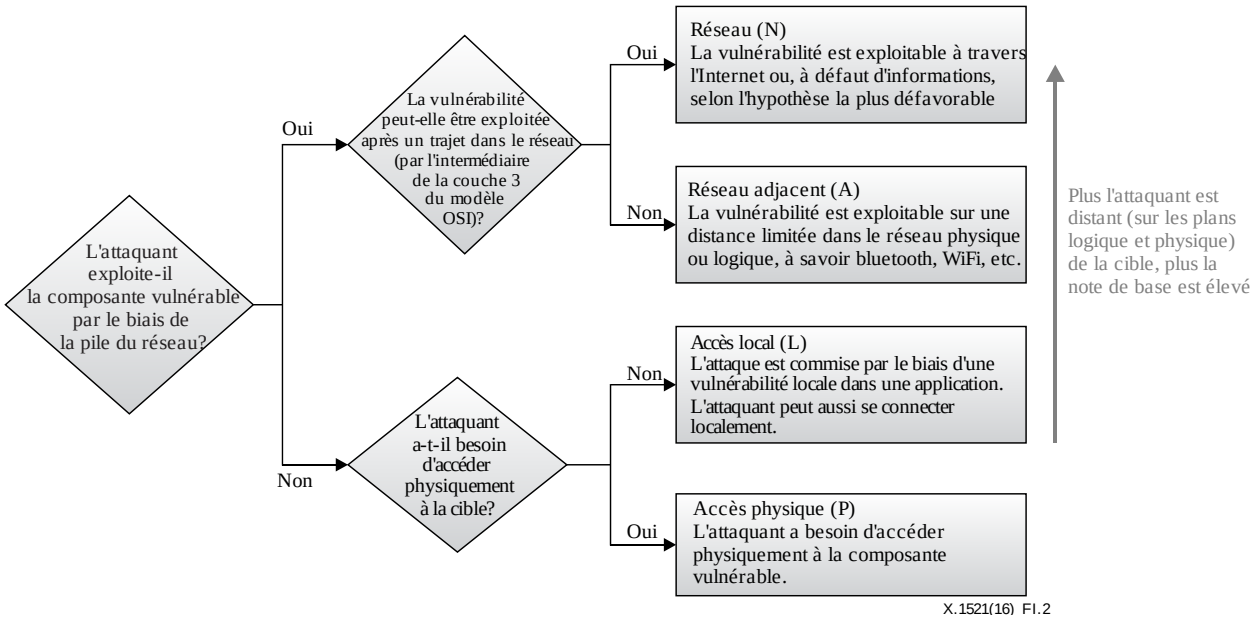
Enchaînement des vulnérabilités: L'exploitation séquentielle de vulnérabilités multiples dans le but d'attaquer un système informatique, une ou plusieurs exploitations en bout de chaîne nécessitant la réussite des exploitations précédentes avant de pouvoir réussir à leur tour. Voir aussi la définition disponible à l'adresse suivante: http://cwe.mitre.org/documents/glossary/#Chain.

Composante vulnérable: La composante logicielle (ou matérielle) qui présente la vulnérabilité et à laquelle il devrait être apporté un correctif.

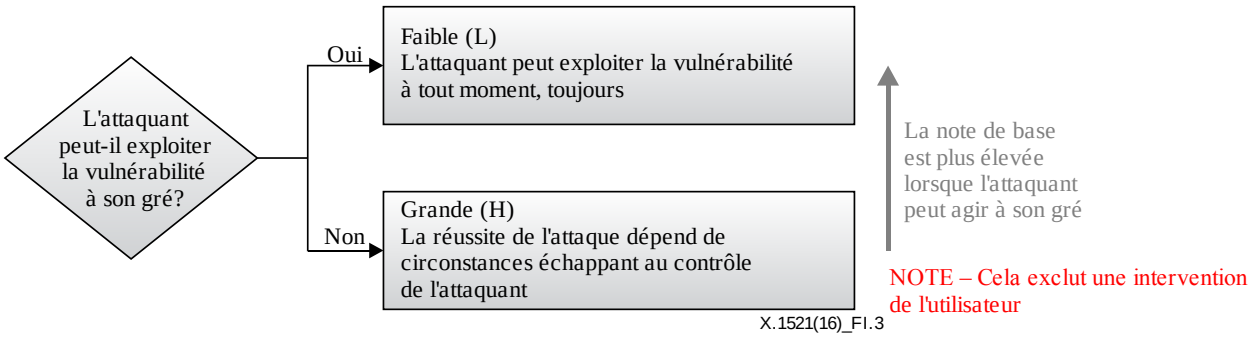
I.5 Rubrique sur l'évaluation

La rubrique sur l'évaluation est un outil de référence rapide destiné à l'évaluation des vulnérabilités dans la version 3.0. Elle vise à compléter les analyses existantes sur l'évaluation qui figurent dans le document de spécification.

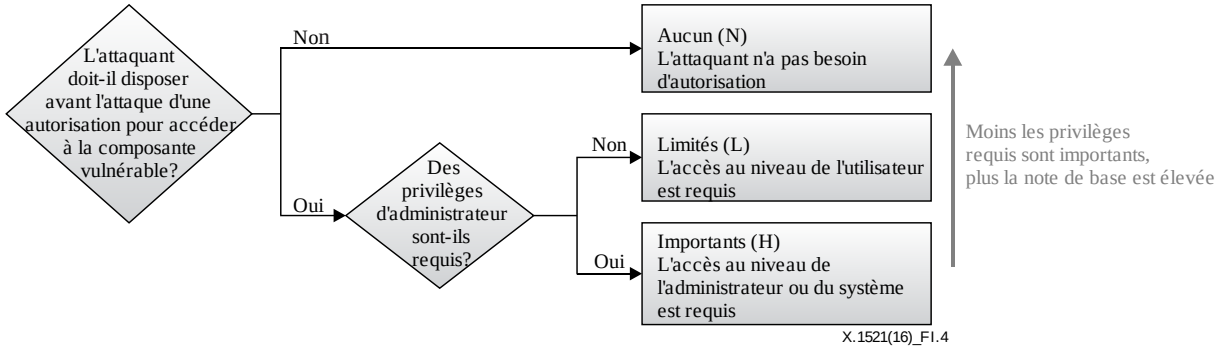
I.5.1 Vecteur de l'attaque



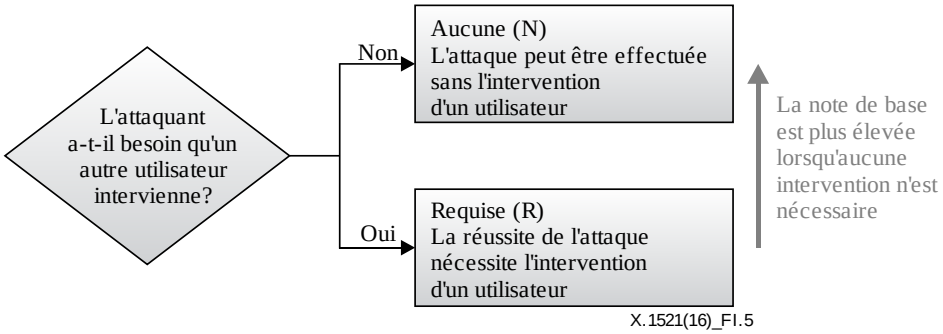
I.5.2 Complexité de l'attaque



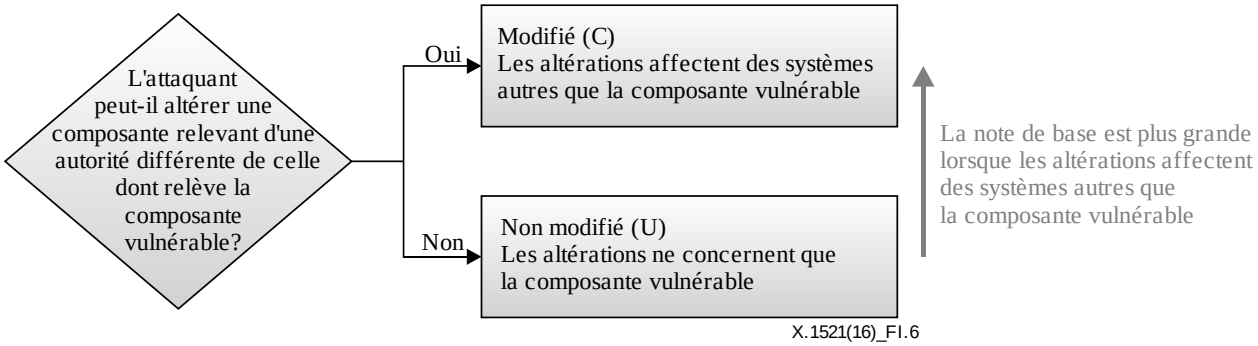
I.5.3 Privilèges requis



I.5.4 Intervention de l'utilisateur

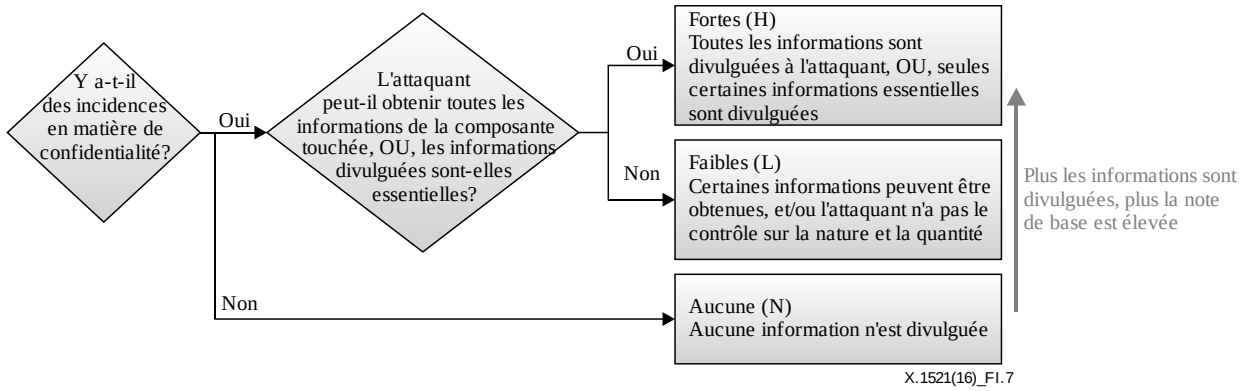


I.5.5 Champ

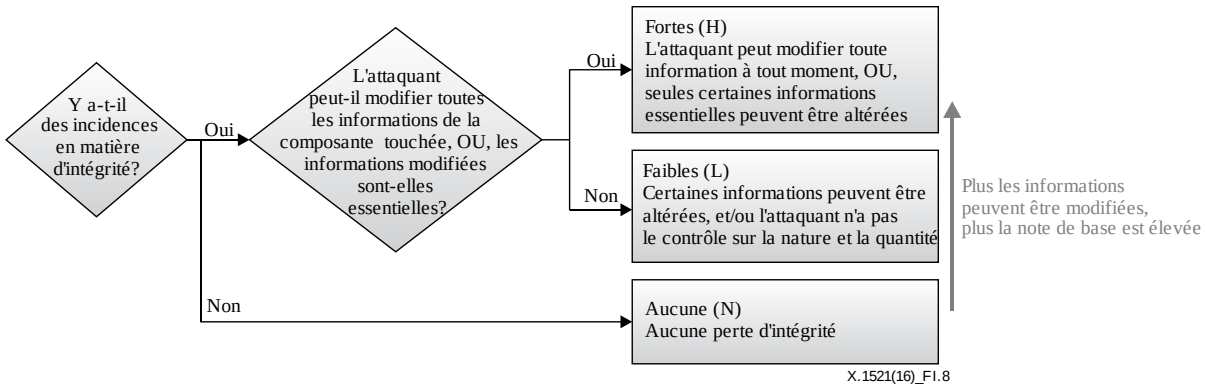


NOTE – Il convient de noter que si une modification du champ ne s'est pas produite, les incidences en matière de confidentialité, d'intégrité et de disponibilité rendent compte des conséquences pour la composante vulnérable, sinon elles rendent compte des conséquences pour la composante qui a subi les plus fortes incidences.

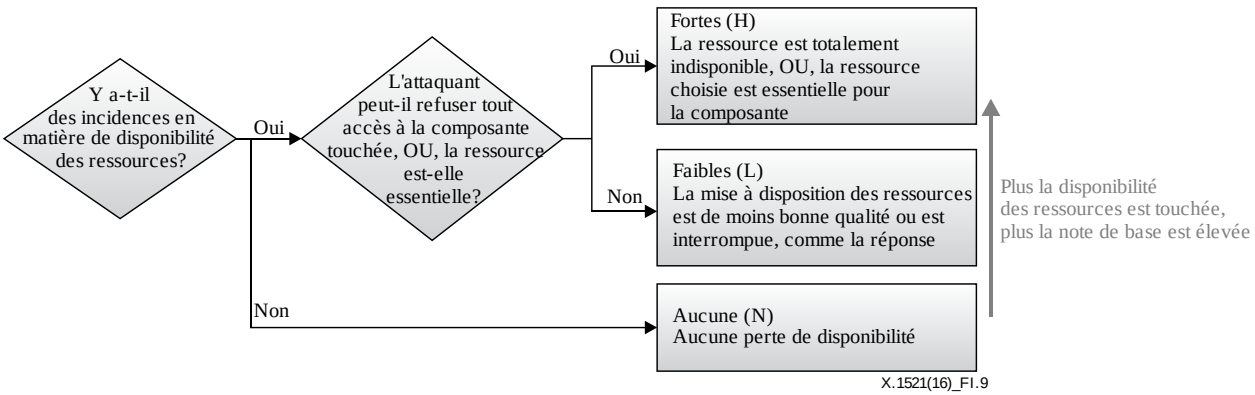
I.5.6 Incidences en matière de confidentialité



I.5.7 Incidences en matière d'intégrité



I.5.8 Incidences en matière de disponibilité



Appendice II

Ressources et liens

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

Ci-après sont mentionnées des références utiles à d'autres documents sur le système CVSS version 3.0.

Ressource	Emplacement
Document de spécification	Contient des descriptions des mesures, des formules et des chaînes vectorielles, disponibles à l'adresse: http://www.first.org/cvss/specification-document
Manuel d'utilisateur	Contient des analyses plus détaillées du système CVSS version 3.0, une rubrique sur l'évaluation et un glossaire, disponibles à l'adresse: http://www.first.org/cvss/user-guide
Document d'exemples	Contient des exemples d'évaluation au moyen du système CVSS version 3.0, disponibles à l'adresse: https://www.first.org/cvss/examples
Logo du système CVSS version 3.0	Images en basse et en haute résolution, disponibles à l'adresse: http://www.first.org/cvss/identity
Calculateur du système CVSS version 3.0	Mise en oeuvre de référence des équations du système CVSS version 3.0, disponible à l'adresse: http://www.first.org/cvss/calculator/3.0
Schéma XML	Définition du schéma, disponible à l'adresse: https://www.first.org/cvss/cvss-v3.0.xsd

Bibliographie

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

[b-UIT-T X.1524] Recommandation UIT-T X.1524 (mars 2011), *Liste des failles courantes.*

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	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, 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, 2017