

Union internationale des télécommunications

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**X.1521**

(04/2011)

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**

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
<b>Echange concernant les vulnérabilités/les états</b>	<b>X.1520–X.1539</b>
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

# Recommandation UIT-T X.1521

## Système d'évaluation des vulnérabilités courantes

### 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
1.0	ITU-T X.1521	2011-04-20	17

## AVANT-PROPOS

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

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

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

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

## NOTE

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

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

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2012

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

## TABLE DES MATIÈRES

	<b>Page</b>
1	Domaine d'application ..... 1
2	Références..... 1
3	Définitions ..... 1
3.1	Termes définis ailleurs ..... 1
3.2	Termes définis dans la présente Recommandation ..... 1
4	Abréviations et acronymes ..... 2
5	Conventions ..... 2
6	Utilisation du CVSS ..... 2
6.1	Description du CVSS ..... 3
6.2	Fonctionnement du CVSS ..... 4
6.3	Notation du CVSS ..... 4
6.4	Utilisateurs du CVSS..... 5
6.5	Groupes de métriques – Métriques de base ..... 5
6.6	Métrique temporelle ..... 9
6.7	Métrique environnementale..... 11
6.8	Vecteurs de base, temporels, environnementaux ..... 14
6.9	Notation – Directives..... 14
6.10	Equations ..... 16
7	Ressources additionnelles ..... 18
Appendice I – Exemples d'usage de CVSS..... 19	
I.1	CVE-2002-0392 ..... 19
I.2	CVE-2003-0818 ..... 20
I.3	CVE-2003-0062 ..... 22
Appendice II – Ressources additionnelles ..... 24	
Bibliographie..... 25	

## **Introduction**

La gestion des TIC nécessite d'identifier et d'évaluer les vulnérabilités touchant de nombreuses plates-formes matérielles et logicielles disparates. Il faut ensuite classer ces vulnérabilités par ordre de priorité et remédier à celles qui présentent les plus grands risques. Lorsqu'il faut remédier à un grand nombre de vulnérabilités, chaque vulnérabilité étant évaluée par rapport à différentes échelles, les gestionnaires de TIC s'en remettent à leurs propres méthodologies pour trouver des moyens de comparer des vulnérabilités disparates et de les traduire en informations décisionnelles.

Du fait que le CVSS normalise l'approche de la caractérisation des vulnérabilités, les utilisateurs du CVSS peuvent invoquer des métriques temporelles et environnementales pour appliquer des informations contextuelles qui reflètent de manière plus précise le risque pour leur environnement unique. Ils peuvent ainsi prendre des décisions mieux informées lorsqu'ils essayent d'atténuer les risques posés par des vulnérabilités agnostiques d'éditeurs dans leur environnement unique.

Sur le plan technique, la présente Recommandation est équivalente et compatible avec le système d'évaluation des vulnérabilités courantes (CVSS) version 2, 20 juin 2007, que l'on peut trouver sur le site Internet à l'adresse <http://www.first.org/cvss>.

# Recommandation UIT-T X.1521

## Système d'évaluation des vulnérabilités courantes

### 1 Domaine d'application

La présente Recommandation propose une approche normalisée pour la communication des caractéristiques et des impacts des vulnérabilités TIC au moyen de métriques temporelles et environnementales qui appliquent des informations contextuelles afin de refléter avec davantage de précision le risque pour chaque environnement unique d'utilisateur.

Sur le plan technique, cette Recommandation est équivalente et compatible avec le "système d'évaluation des vulnérabilités courantes (CVSS), version 2", 20 juin 2007, que l'on trouve sur le site internet à l'adresse <http://www.first.org/cvss>.

### 2 Références

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

[CVSS Guide] CVSS (2007), *A complete Guide to the Common Vulnerability Scoring System Version 2.0*.  
<<http://www.first.org/cvss/cvss-guide.pdf>>

### 3 Définitions

#### 3.1 Termes définis ailleurs

**3.1.1 vulnérabilité** [b-UIT-T X.1500]: toute faiblesse qui pourrait être exploitée pour vider 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**: aptitude d'un sujet à voir, modifier ou communiquer avec un objet. L'accès permet le flux d'informations entre le sujet et l'objet.

**3.2.2 disponibilité**: c'est l'accès fiable et en temps utile par des personnes autorisées à des données et des ressources.

**3.2.3 confidentialité**: principe de sécurité qui fonctionne pour veiller à ce que l'information ne soit pas divulguée à des sujets non autorisés.

**3.2.4 intégrité**: principe de sécurité qui veille à ce que l'information et les systèmes ne soient pas modifiés de façon malveillante ou accidentelle.

**3.2.5 risque**: impact relatif qu'une vulnérabilité exploitée aurait sur un environnement utilisateur.

**3.2.6 menace**: probabilité ou fréquence d'un événement dangereux.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

A	impact sur la disponibilité ( <i>availability impact</i> )
AC	complexité de l'accès ( <i>access complexity</i> )
AR	exigence de disponibilité ( <i>availability requirement</i> )
Au	authentification ( <i>authentication</i> )
AV	vecteur d'accès ( <i>access vector</i> )
C	impact sur la confidentialité ( <i>confidentiality impact</i> )
CDP	possibilité de dommage collatéral ( <i>collateral damage potential</i> )
CR	exigence de confidentialité ( <i>confidentiality requirement</i> )
CVSS	système d'évaluation des vulnérabilités courantes ( <i>common vulnerability scoring system</i> )
DMA	accès à la mémoire directe ( <i>direct memory access</i> )
DNS	système de nom de domaine ( <i>domain name system</i> )
E	impact sur l'exploitabilité ( <i>exploitability impact</i> )
I	impact sur l'intégrité ( <i>integrity impact</i> )
IM	messagerie instantanée ( <i>instant messaging</i> )
IR	exigence d'intégrité ( <i>integrity requirement</i> )
JVN	Japan Vulnerability Notes
NVD	National Vulnerability Database
RC	niveau de confiance ( <i>report confidence</i> )
RL	niveau de correction ( <i>remediation level</i> )
RPC	appel de procédure éloigné ( <i>remote procedure call</i> )
SLA	accord de niveau de service ( <i>service level agreement</i> )
TD	distribution de cibles ( <i>target distribution</i> )
TIC	technologies de l'information et de la communication
USB	bus série universel ( <i>universal serial bus</i> )

## 5 Conventions

Néant.

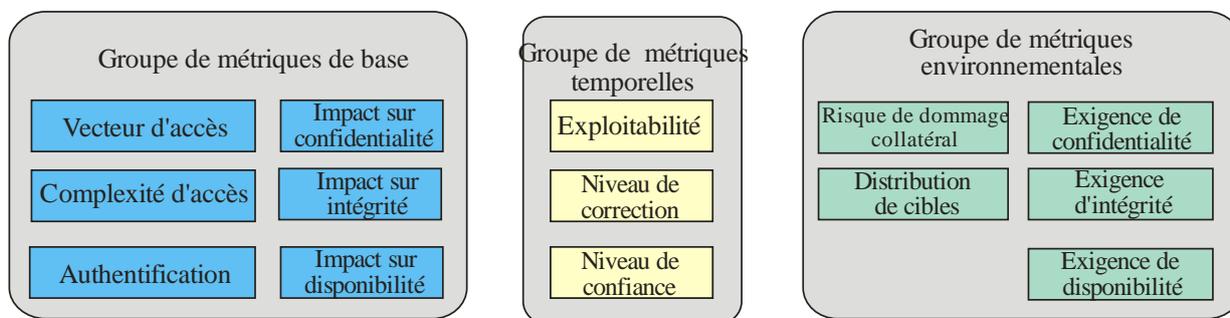
## 6 Utilisation du CVSS

Actuellement, la gestion des TIC nécessite d'identifier et d'évaluer les vulnérabilités touchant de nombreuses plates-formes matérielles et logicielles disparates. Il faut ensuite classer ces vulnérabilités par ordre de priorité et remédier à celles qui présentent les plus grands risques. Lorsqu'il faut remédier à un grand nombre de vulnérabilités, chaque vulnérabilité étant évaluée par rapport à différentes échelles, il est difficile pour les gestionnaires de TIC de traduire cette accumulation de données sur la vulnérabilité en informations décisionnelles. Le système d'évaluation des vulnérabilités courantes (CVSS) est un cadre ouvert qui traite de cette question. Il offre les avantages suivants:

- Notation normalisée des vulnérabilités: lorsqu'une organisation normalise l'évaluation des vulnérabilités sur l'ensemble de ses plates-formes logicielles et matérielles, elle peut s'appuyer sur une politique de gestion unique des vulnérabilités. Cette politique peut être similaire à un accord de niveau de service (SLA, *service level agreement*) qui définit comment une vulnérabilité particulière doit être validée et corrigée rapidement.
- Cadre ouvert: les utilisateurs peuvent ressentir une certaine confusion lorsqu'une notation arbitraire est attribuée à une vulnérabilité. "Quelles sont les propriétés qui sont à l'origine de cette notation?" "En quoi est-elle différente de celle diffusée hier?". Avec le CVSS, chacun peut voir les caractéristiques individuelles utilisées pour établir une évaluation.
- Risques prioritaires: lorsque l'évaluation environnementale est calculée, la vulnérabilité devient alors contextuelle. C'est-à-dire que les évaluations des vulnérabilités représentent désormais le risque courant pour une organisation. Les utilisateurs connaissent l'importance d'une vulnérabilité donnée dans sa relation avec d'autre vulnérabilité.

## 6.1 Description du CVSS

Le CVSS se compose de trois groupes de métriques: base, temporelle et environnementale, qui consistent chacun en un ensemble de métriques comme indiqué à la Figure 1.



X.1521(11)\_FC1

**Figure 1 – Groupes de métriques CVSS**

Ces groupes de métriques sont décrits ci-après:

- Base: ce groupe représente les caractéristiques intrinsèques et fondamentales d'une vulnérabilité qui sont constantes dans le temps et dans les environnements utilisateurs. Les métriques de base sont étudiées au paragraphe 6.5.
- Temporelle: ce groupe représente les caractéristiques d'une vulnérabilité qui changent dans le temps mais pas entre les environnements utilisateurs. Les métriques temporelles sont examinées au paragraphe 6.6.
- Environnementale: ce groupe représente les caractéristiques d'une vulnérabilité qui sont pertinentes et uniques à un environnement utilisateur particulier. Les métriques environnementales sont examinées au paragraphe 6.7.

L'objet du groupe de base CVSS est de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité. Cette approche objective retenue pour caractériser des vulnérabilités fournit aux utilisateurs une représentation claire et intuitive d'une vulnérabilité. Les utilisateurs peuvent alors invoquer les groupes temporels et environnementaux pour fournir des informations contextuelles qui reflètent avec davantage de précision le risque pour leur environnement unique. Cela leur permet de prendre des décisions mieux informées lorsqu'ils essaient d'atténuer des risques posés par les vulnérabilités.

## 6.2 Fonctionnement du CVSS

Lorsque des valeurs sont attribuées aux métriques de base, l'équation de base calcule une évaluation allant de zéro à dix puis un vecteur est créé comme illustré ci-dessous à la Figure 2. Ce vecteur facilite la nature "ouverte" du cadre. C'est une chaîne de texte qui contient les valeurs attribuées à chaque métrique et elle sert à communiquer exactement comment on déduit l'évaluation pour chaque vulnérabilité. Ce vecteur doit donc toujours être affiché avec la note de vulnérabilité. Les vecteurs sont expliqués plus en détail au paragraphe 7.4.

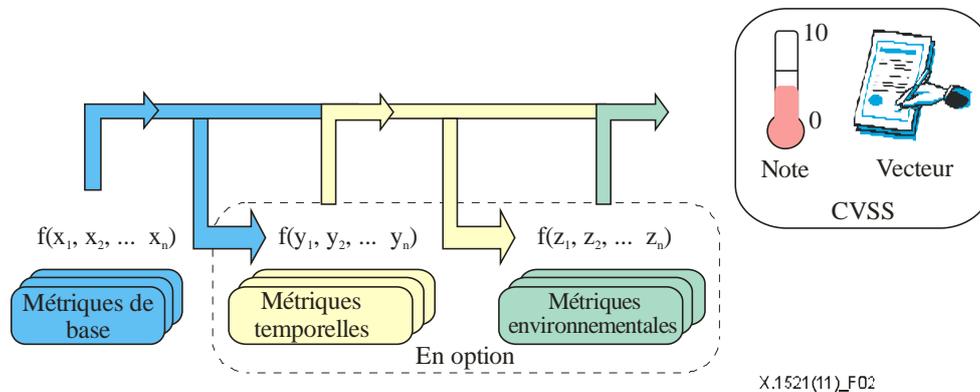


Figure 2 – Métriques et équations du CVSS

Si on le souhaite, on peut affiner l'évaluation de base en attribuant des valeurs aux métriques temporelles et environnementales. Cela est utile pour offrir un contexte additionnel à une vulnérabilité en reflétant de façon plus précise le risque posé par la vulnérabilité à l'environnement d'un utilisateur. Toutefois, cela n'est pas requis. En fonction de l'objectif de chacun, la note de base et le vecteur peuvent suffire.

Si l'on a besoin d'une note temporelle, l'équation temporelle combinera les métriques temporelles à la note de base pour produire une note temporelle allant de 0 à 10. De même, si une note environnementale est nécessaire, l'équation environnementale combinera les métriques environnementales et la note temporelle pour produire une évaluation environnementale allant de 0 à 10. Les équations de base, temporelles et environnementales sont décrites en détail au paragraphe 8.2.

## 6.3 Notation du CVSS

Généralement, les métriques de base et temporelles sont spécifiées par des analystes du bulletin des vulnérabilités, les fabricants de produits de sécurité ou les éditeurs d'applications car ils disposent généralement de meilleures informations sur les caractéristiques d'une vulnérabilité par rapport aux utilisateurs. Les métriques environnementales sont toutefois spécifiées par les utilisateurs qui sont les mieux placés pour évaluer l'impact potentiel d'une vulnérabilité sur leurs propres environnements.

## 6.4 Utilisateurs du CVSS

De nombreuses organisations utilisent le CVSS et chacune d'entre elles y trouve un intérêt différent. Voici quelques exemples:

- Fournisseurs de bulletins de vulnérabilités: des organisations à but non lucratif et des organisations commerciales établissent des notes de base et temporelles de CVSS ainsi que des vecteurs dans leurs bulletins de vulnérabilités gratuits. Ces bulletins offrent beaucoup d'informations, y compris des dates de découverte, sur les systèmes affectés et les liens avec les fabricants pour des recommandations relatives à des correctifs.
- Editeurs d'applications logicielles: les éditeurs d'applications logicielles fournissent des notes de base et des vecteurs CVSS à leurs clients. Cela les aide à communiquer correctement sur la gravité des vulnérabilités dans leurs produits et aide leurs clients à gérer avec efficacité leurs risques TIC.
- Organisations d'utilisateurs: de nombreuses organisations du secteur privé utilisent le CVSS, en interne, pour prendre des décisions en toute connaissance de cause en matière de gestion des vulnérabilités. Elles utilisent des scanners ou des technologies de contrôle pour, tout d'abord, localiser l'hôte et les vulnérabilités des applications. Elles combinent ces données avec des notes de base CVSS, temporelles et environnementales pour obtenir davantage d'informations contextuelles sur les risques et remédient aux vulnérabilités qui posent les plus grands risques pour leurs systèmes.
- Analyse et gestion des vulnérabilités: les organisations de gestion des vulnérabilités analysent les réseaux en ce qui concerne les vulnérabilités TIC. Elles donnent des notes de base CVSS pour toutes les vulnérabilités sur chaque machine hôte. Les organisations d'utilisateurs utilisent ce flux de données critiques pour gérer avec davantage d'efficacité leurs infrastructures TIC en réduisant les pannes et en les protégeant contre des menaces malveillantes ou des menaces d'accidents TIC.
- Gestion de la sécurité (risque): les entreprises de gestion des risques de sécurité utilisent les notes CVSS comme informations d'entrée pour calculer un risque organisationnel ou un niveau de menace. Les entreprises utilisent des applications complexes qui, souvent, intègrent les données d'une topologie de réseau d'organisation, des données de vulnérabilité, une base d'actifs pour fournir à leurs clients une perspective mieux documentée de leur niveau de risque.
- Chercheurs: le cadre ouvert du CVSS permet d'effectuer des recherches à des fins d'analyse de statistiques et de vulnérabilités.

## 6.5 Groupes de métriques – Métriques de base

Le groupe des métriques de base capture les caractéristiques d'une vulnérabilité qui sont constantes dans le temps et dans les environnements utilisateurs. Le vecteur d'accès, la complexité d'accès et les métriques d'authentification capturent comment on accède à la vulnérabilité et déterminent si les conditions sont requises ou non pour exploiter cette vulnérabilité. Les trois métriques d'impact mesurent comment une vulnérabilité, si elle est exploitée, affectera directement un actif TIC, où les impacts sont définis indépendamment comme le degré de perte de confidentialité, d'intégrité et de disponibilité. Par exemple, une vulnérabilité pourrait causer une perte partielle de l'intégrité et de la disponibilité mais aucune perte de confidentialité.

### 6.5.1 Vecteur d'accès (AV)

Cette métrique indique comment la vulnérabilité est exploitée. Les valeurs possibles de cette métrique sont récapitulées dans le Tableau 1. Plus éloigné est un attaquant qui vise un système hôte, plus élevée est la note de vulnérabilité.

**Tableau 1 – Evaluation du vecteur d'accès**

Valeur de la métrique	Description
Local (L)	Une vulnérabilité exploitable avec un accès local uniquement exige que l'attaquant ait soit un accès physique au système vulnérable soit un compte local (coque). Les attaques périphériques comme les pare-feux/USB DMA et les escalades de privilèges locaux (par exemple sudo) sont des exemples de vulnérabilités exploitables localement.
Réseau adjacent (A)	Une vulnérabilité exploitable avec un accès réseau adjacent exige que l'attaquant ait accès soit à la radiodiffusion soit à un domaine de collision du logiciel vulnérable. Les réseaux secondaires IP locaux, Bluetooth, IEEE 802.11, et le segment Ethernet local sont des exemples de réseaux locaux.
Réseau (N)	Une vulnérabilité exploitable avec un accès réseau signifie que le logiciel vulnérable est lié à la pile du réseau et que l'attaquant n'a pas besoin d'accès réseau local ou d'accès local. Une telle vulnérabilité est souvent appelée "exploitable à distance". Un débordement de mémoire RPC est un exemple d'attaque de réseau.

### 6.5.2 Complexité d'accès (AC)

Cette métrique mesure la complexité de l'impact requise pour exploiter la vulnérabilité lorsqu'un attaquant a obtenu l'accès au système visé. Par exemple, considérons un débordement de mémoire dans un service internet: lorsque le système visé est localisé, l'attaquant peut lancer une attaque comme il le veut.

Toutefois, d'autres vulnérabilités peuvent nécessiter des étapes additionnelles pour être exploitées. Par exemple, la vulnérabilité dans un courriel client n'est exploitée qu'après que l'utilisateur ait téléchargé et ouvert une pièce jointe contaminée. Les valeurs possibles de cette métrique sont énumérées au Tableau 2. Plus faible est la complexité requise, plus élevée est la note de la vulnérabilité.

**Tableau 2 – Evaluation de la complexité d'accès**

Valeur de la métrique	Description
Elevée (H)	Des conditions d'accès spécialisées existent. Par exemple: <ul style="list-style-type: none"> <li>• Dans la plupart des configurations, la partie qui attaque doit déjà avoir des privilèges élevés ou des systèmes additionnels de "bluff" en plus du système d'attaque (par exemple, piratage DNS).</li> <li>• L'attaque dépend des méthodes d'ingénierie sociale qui seraient facilement détectées par des connaisseurs. Par exemple, la victime doit effectuer plusieurs actions suspectes ou atypiques.</li> <li>• La configuration vulnérable est très rare en pratique.</li> <li>• S'il existe une condition de course, la fenêtre est très étroite.</li> </ul>

**Tableau 2 – Evaluation de la complexité d'accès**

Valeur de la métrique	Description
Moyenne (M)	<p>Les conditions d'accès sont quelque peu spécialisées; voici des exemples:</p> <ul style="list-style-type: none"> <li>• La partie qui attaque est limitée à un groupe de systèmes ou d'utilisateurs à un niveau quelconque d'autorisation, éventuellement, sans confiance.</li> <li>• Des informations doivent être rassemblées avant qu'une attaque puisse être lancée avec succès.</li> <li>• La configuration affectée n'est pas une configuration par défaut et elle est couramment configurée (par exemple, une vulnérabilité présente lorsqu'un serveur effectue l'authentification d'un compte utilisateur via un schéma spécifique, mais elle n'est pas présente pour un autre schéma d'authentification).</li> <li>• L'attaque exige un petit volume d'ingénierie sociale qui pourrait parfois tromper des utilisateurs prudents (par exemple, attaques d'hameçonnage qui modifient la barre de statut d'un navigateur internet pour montrer un lien faux, devoir être sur une liste d'amis avant d'envoyer un exploit IM).</li> </ul>
Faible visite (L)	<p>Il n'existe pas de condition d'accès spécialisée ou de circonstances atténuantes. Voici quelques exemples:</p> <ul style="list-style-type: none"> <li>• Le produit affecté nécessite généralement l'accès à une large gamme de systèmes et d'utilisateurs, éventuellement anonymes et non fiables (par exemple, web internet ou serveur de courrier).</li> <li>• La configuration affectée est par défaut ou universelle.</li> <li>• L'attaque peut être faite manuellement et demande peu de compétences ou peu d'informations supplémentaires.</li> <li>• La condition de course est facile (c'est-à-dire qu'il s'agit techniquement d'une course mais qu'on peut la gagner facilement).</li> </ul>

### 6.5.3 Authentification (Au)

Cette métrique mesure le nombre de fois qu'un attaquant doit s'authentifier à une cible pour exploiter une vulnérabilité. Cette métrique n'évalue pas la force ou la complexité du processus d'authentification mais seulement qu'un attaquant est invité à fournir des références avant qu'un exploit se produise. Les valeurs possibles de cette métrique sont récapitulées au Tableau 3. Moins est élevé le nombre d'instances d'authentification requises, plus élevée est la note de la vulnérabilité.

**Tableau 3 – Evaluation des notes de l'authentification**

Valeur de la métrique	Description
Multiple (M)	L'exploitation d'une vulnérabilité exige que l'attaquant s'authentifie deux ou plusieurs fois, même si les mêmes références sont utilisées chaque fois. Un exemple serait celui d'un attaquant s'authentifiant face à un système d'exploitation en plus de fournir des références pour accéder à une application hébergée par ce système.
Unique (S)	Cette vulnérabilité exige qu'un attaquant soit connecté au système (comme, par exemple, sur une ligne de commande ou via une session d'ordinateur de bureau ou une interface web).
Aucune (N)	L'authentification n'est pas requise pour exploiter la vulnérabilité.

La métrique doit être appliquée en se basant sur l'authentification que l'attaquant exige avant de lancer une attaque. Par exemple, si un serveur de courrier est vulnérable à une commande qui peut être lancée avant qu'un utilisateur s'authentifie, la métrique doit être classée comme "aucune"

puisque l'attaquant peut lancer l'exploit avant que les références soient requises. Si la commande vulnérable n'est disponible qu'après une authentification réussie, la vulnérabilité doit alors être notée comme "unique" ou "multiple" en fonction du nombre d'instances d'authentification avant de lancer la commande.

#### 6.5.4 Impact sur la confidentialité (C)

Cette métrique mesure l'impact d'une vulnérabilité exploitée avec succès sur la confidentialité. La confidentialité consiste à limiter l'accès à l'information et à la divulgation à des utilisateurs autorisés seulement, ainsi que d'empêcher l'accès ou la divulgation à des utilisateurs non autorisés. Les valeurs possibles de cette métrique sont récapitulées au Tableau 4. L'augmentation de l'impact sur la confidentialité augmente la note de la vulnérabilité.

**Tableau 4 – Evaluation de la notation de l'impact sur la confidentialité**

Valeur de la métrique	Description
Aucune (N)	Il n'y a pas d'impact sur la confidentialité du système.
Partielle (P)	Il y a une divulgation considérable de l'information. L'accès à certains fichiers du système est possible mais l'attaquant n'a pas le contrôle sur ce qui est obtenu ou sur l'importance de la perte encourue. La vulnérabilité qui ne divulgue que certains tableaux d'une base de données est un exemple.
Complète (C)	Il y a une divulgation totale de l'information et il en résulte que tous les fichiers du système sont révélés. L'attaquant peut lire toutes les données du système (mémoire, fichiers, etc.).

#### 6.5.5 Impact sur l'intégrité (I)

Cette métrique mesure l'impact d'une vulnérabilité exploitée avec succès sur l'intégrité. L'intégrité se réfère à la confiance et à la véracité garantie des informations. Les valeurs possibles de cette métrique sont récapitulées au Tableau 5. L'augmentation de l'impact sur l'intégrité augmente la note de la vulnérabilité.

**Tableau 5 – Evaluation de la note de l'impact sur l'intégrité**

Valeur de la métrique	Description
Aucune (N)	Il n'y a pas d'impact sur l'intégrité du système.
Partielle (P)	La modification de certains fichiers système ou d'informations est possible mais l'attaquant n'a pas le contrôle sur ce qui peut être modifié ni sur la portée de ce que l'attaquant peut affecter. Par exemple, des fichiers système ou d'applications peuvent être écrasés ou modifiés mais soit l'attaquant n'a pas le contrôle sur le choix des fichiers qui sont affectés soit il peut modifier des fichiers dans un domaine ou un contexte limité seulement.
Complète (C)	Il y a une compromission totale de l'intégrité du système. Il y a perte complète du système de protection. Il en résulte que l'ensemble du système est compromis. L'attaquant peut modifier n'importe quel fichier sur le système visé.

### 6.5.6 Impact sur la disponibilité (A)

Cette métrique mesure l'impact d'une vulnérabilité exploitée avec succès sur la disponibilité. La disponibilité se réfère à l'accessibilité des ressources d'informations. Les attaques qui endommagent la bande passante d'un réseau, les cycles des processeurs ou les espaces sur le disque ont toutes un impact sur la disponibilité d'un système. Les valeurs possibles de cette métrique sont récapitulées au Tableau 6. L'augmentation de l'impact sur la disponibilité augmente la note de la vulnérabilité.

**Tableau 6 – Evaluation de la note de l'impact sur la disponibilité**

Valeur de la métrique	Description
Aucune (N)	Il n'y a pas d'impact sur la disponibilité du système.
Partielle (P)	On note une performance réduite ou des interruptions en matière de disponibilité des ressources. Une succession de requêtes basée sur un réseau qui permet un nombre limité de connexions réussies à un service internet est un exemple.
Complète (C)	Il y a arrêt total des ressources affectées. L'attaquant peut rendre ces ressources totalement indisponibles.

## 6.6 Métrique temporelle

La menace posée par une vulnérabilité peut évoluer dans le temps. La confirmation des détails techniques d'une vulnérabilité, l'état du remède de la vulnérabilité et la disponibilité du code d'exploit ou des techniques sont trois facteurs que le CVSS capture. La métrique temporelle étant en option, elle inclut une valeur de métrique qui n'a aucun effet sur la note. Cette valeur est utilisée lorsque l'utilisateur estime que cette métrique particulière ne s'applique pas et qu'il souhaite la "sauter".

### 6.6.1 Potentiel d'exploitation (E)

Cette métrique mesure l'état actuel des techniques d'exploitation ou la disponibilité des codes. La disponibilité publique de codes d'exploitation faciles à utiliser augmente le nombre d'attaquants potentiels en incluant ceux qui ne sont pas compétents, ce qui augmente la gravité de la vulnérabilité.

Initialement, l'exploitation dans le réel peut n'être que théorique. La publication de codes dont la faisabilité a été démontrée, de codes d'exploitation fonctionnelle ou de détails techniques suffisants et nécessaires pour exploiter la vulnérabilité peut suivre. En outre, le code d'exploitation disponible peut évoluer d'une démonstration de faisabilité jusqu'au code d'exploitation qui réussit à exploiter le code qui parvient à exploiter la vulnérabilité avec cohérence. Dans les cas graves, il peut être fourni sous la forme de la charge utile d'un ver ou d'un virus basé sur le réseau. Les valeurs possibles de cette métrique sont récapitulées au Tableau 7. Plus une vulnérabilité peut être exploitée facilement, plus élevée est la note de la vulnérabilité.

**Tableau 7 – Evaluation de la note de l'impact sur l'exploitabilité**

<b>Valeur de la métrique</b>	<b>Description</b>
Non prouvée (U)	Aucun code d'exploitation n'est disponible ou bien un exploit est entièrement théorique.
Démonstration de faisabilité (POC)	Le code d'exploitation de la démonstration de faisabilité d'une attaque qui n'est pas pratique pour la plupart des systèmes est disponible. Le code ou la technique ne sont pas fonctionnels dans toutes les situations et peuvent nécessiter une modification substantielle réalisée par un attaquant compétent.
Fonctionnelle (F)	Le code d'exploitation fonctionnel est disponible. Ce code travaille dans la plupart des situations où existe une vulnérabilité.
Elevée (H)	Soit la vulnérabilité est exploitable par un code autonome mobile fonctionnel, soit aucun exploit n'est requis (déclenchement manuel) et les détails sont largement disponibles. Le code travaille dans toutes les situations ou est activement fourni via un agent autonome mobile (comme un ver ou un virus).
Indéfinie (ND)	L'attribution de cette valeur à la métrique n'aura aucune influence sur la note. C'est un signal adressé à l'équation pour "sauter" cette métrique.

### 6.6.2 Niveau de correction (RL)

Le niveau de correction d'une vulnérabilité est un facteur important pour la fixation des priorités. La vulnérabilité type n'est pas corrigée lorsqu'elle est publiée la première fois. Les solutions de repli et les réparations peuvent constituer des remèdes provisoires jusqu'à ce qu'un correctif officiel ou une mise à hauteur soient diffusés. Chacun de ces stades respectifs ajuste la note temporelle vers le bas, traduisant ainsi l'urgence qui diminue alors que le remède devient final. Les valeurs possibles de cette métrique sont récapitulées au Tableau 8. Moins un remède est officiel et permanent, plus élevée est la note de vulnérabilité.

**Tableau 8 – Evaluation de la note du niveau de correction**

<b>Valeur métrique</b>	<b>Description</b>
Correction officielle (OF)	Il existe une solution complète de l'éditeur. Soit l'éditeur a diffusé un correctif officiel soit il existe une mise à hauteur.
Correction temporaire (TF)	Un correctif officiel mais provisoire est disponible. Cela inclut des instances pour lesquelles l'éditeur diffuse un remède temporaire à chaud, un outil ou une solution de repli.
Solution de repli (W)	C'est une solution officieuse, qui n'est pas proposée par l'éditeur et qui est disponible. Dans certains cas, les utilisateurs de la technologie affectée créent un remède de leur propre ou indiquent les étapes de solutions de repli ou de procédures d'atténuation de la vulnérabilité.
Indisponible (U)	Soit il n'y a pas de solution disponible, soit elles sont impossibles à appliquer.
Indéfinie (ND)	L'attribution de cette valeur à la métrique n'influera pas sur la note. C'est un signal adressé à l'équation pour qu'elle "saute" cette métrique.

### 6.6.3 Niveau de confiance (RC)

Cette métrique mesure le niveau de confiance dans l'existence de la vulnérabilité et dans la crédibilité des détails techniques connus. Parfois, seule l'existence de vulnérabilités est connue mais sans détail spécifique. Des vulnérabilités peuvent être corroborées ultérieurement puis confirmées par l'auteur ou le fabricant de la technologie affectée. L'urgence d'une vulnérabilité est plus élevée lorsque l'on sait qu'elle existe avec certitude. Cette métrique suggère également le niveau de connaissance technique disponible pour des attaquants potentiels. Les valeurs possibles de cette métrique sont récapitulées au Tableau 9. Plus une vulnérabilité est validée par l'éditeur ou par d'autres sources réputées, plus élevée est la note.

**Tableau 9 – Evaluation de la note du niveau de confiance**

Valeur de la métrique	Description
Non confirmée (UC)	Il existe une source non confirmée unique ou, éventuellement, plusieurs rapports se contredisant. La validité des rapports est peu fiable. On citera comme exemple une rumeur émanant de la communauté des pirates.
Non corroborée (UR)	Il existe de multiples sources non officielles, incluant éventuellement des entreprises de sécurité indépendantes ou des organisations de recherche. A ce stade, il y a peut-être des détails techniques contradictoires ou d'autres ambiguïtés en suspens.
Confirmée (C)	La vulnérabilité a été reconnue par l'éditeur ou l'auteur de la technologie affectée. La vulnérabilité peut aussi être confirmée lorsque son existence est confirmée à partir d'un événement externe comme la publication d'un code d'exploit fonctionnel ou d'un code d'exploit la faisabilité a été démontrée ou d'une exploitation large.
Non définie (ND)	L'attribution de cette valeur à la métrique n'aura pas d'influence sur la note. C'est un signal adressé à l'équation pour qu'elle "saute" cette métrique.

## 6.7 Métrique environnementale

Des environnements différents peuvent avoir une immense incidence sur le risque qu'une vulnérabilité pose à une organisation ou à ses parties intéressées. Le groupe "métrique environnementale" CVSS capture les caractéristiques d'une vulnérabilité qui sont associées à l'environnement TIC d'un utilisateur. Vu que les métriques environnementales sont en option, elles comprennent chacune une valeur de métrique qui n'a pas d'effet sur la note. Cette valeur est utilisée lorsque l'utilisateur estime que la métrique donnée ne s'applique pas et qu'il souhaite la "sauter".

### 6.7.1 Dommages collatéraux potentiels (CDP)

Cette métrique mesure le potentiel de perte d'actifs de vie ou d'actifs physiques suite à des dégâts ou des vols de propriétés ou d'équipements. Cette métrique mesure également la perte économique de productivité ou de recettes. Les valeurs possibles de cette métrique sont récapitulées au Tableau 10. Naturellement, plus le dégât potentiel est élevé, plus la note de vulnérabilité est élevée.

**Tableau 10 – Evaluation de la note de dommages collatéraux potentiels**

Valeur de la métrique	Description
Aucune (N)	Il n'y a pas de risque de perte de vie, d'actifs physiques, de productivité ou de revenus.
Faible (L)	Un exploit manqué de cette vulnérabilité peut se traduire par de légers dommages physiques ou à la propriété. Il peut également y avoir une légère perte de revenus ou de productivité pour l'organisation.
Faible-moyenne (LM)	Un exploit réussi de cette vulnérabilité peut se traduire par des dommages moyens physiques ou à la propriété. On peut également constater une perte modérée de revenus ou de productivité pour l'organisation.
Moyenne-élevée (MH)	Un exploit réussi de cette vulnérabilité peut se traduire par des dommages physiques importants ou une perte de biens. Ou bien, on peut constater une perte importante de revenus ou de productivité.
Elevé (H)	Un exploit réussi de cette vulnérabilité peut se traduire par des dommages catastrophiques physiques ou à la propriété ou des pertes. Ou, on peut constater une perte catastrophique de revenus ou de productivité.
Non définie (ND)	L'attribution de cette valeur à la métrique n'aura pas d'influence sur la note. C'est un signal adressé à l'équation pour "sauter" cette métrique.

Il est évident que chaque organisation doit déterminer pour elle-même la signification précise des mots "légère, modérée, importante et catastrophique".

### 6.7.2 Distribution des cibles (TD)

Cette métrique mesure la proportion de systèmes vulnérables. On la considère comme un indicateur lié l'environnement afin de calculer approximativement le pourcentage de systèmes qui pourraient être touchés par la vulnérabilité. Les valeurs possibles de cette métrique sont récapitulées au Tableau 11. Plus est élevée la proportion de systèmes vulnérables, plus est élevée la note.

**Tableau 11 – Evaluation de la note de la distribution des cibles**

Valeur de la métrique	Description
Aucune (N)	Il n'existe aucun système de cible ou bien les cibles sont tellement spécialisées qu'elles n'existent simplement que dans un montage de laboratoire. Effectivement, 0% de cet environnement est risqué.
Faible (L)	Les cibles existent à l'intérieur de l'environnement mais sur une petite échelle. Entre 1% et 25% de l'ensemble de l'environnement sont exposés à un risque.
Moyenne (M)	Les cibles existent à l'intérieur de l'environnement mais sur une échelle moyenne. Entre 26% et 75% de l'ensemble de l'environnement sont exposés à un risque.
Elevée (H)	Les cibles existent à l'intérieur de l'environnement mais sur l'échelle considérable. Entre 60% et 100% de l'ensemble de l'environnement sont exposés à un risque.
Indéfinie (ND)	L'assignation de cette valeur à la métrique n'aura pas d'influence sur la note. C'est un signal adressé à l'équation pour "sauter" cette métrique.

### 6.7.3 Conditions de sécurité (CR, IR, AR)

Ces métriques permettent à un analyste de personnaliser la notation CVSS en fonction de l'importance des actifs TIC affectés d'une organisation d'utilisateurs, mesurée en termes de confidentialité, d'intégrité et de disponibilité. C'est-à-dire que si des actifs TIC supportent une fonction d'entreprise pour laquelle la disponibilité est la plus importante, l'analyste peut attribuer une valeur plus élevée à la disponibilité, par rapport à la confidentialité et à l'intégrité. Chaque condition de sécurité correspond à trois valeurs possibles: faible, moyenne ou élevée.

L'effet total sur la note environnementale est déterminé par la métrique d'impact de base correspondant (il est à noter que la confidentialité de base, l'intégrité et la métrique d'impact sur la disponibilité ne sont pas modifiées). Cela veut dire que ces métriques modifient la note environnementale en pondérant de nouveau la confidentialité, l'intégrité et la disponibilité. Par exemple, l'impact sur la confidentialité a une pondération augmentée si les conditions de sécurité sont élevées (CR). De même, la métrique d'impact de confidentialité a un poids diminué si la condition de confidentialité est basse. La métrique d'impact de confidentialité est neutre si la condition de confidentialité est moyenne. Cette même logique s'applique aux exigences d'intégrité et de disponibilité.

Il est à noter que la condition de confidentialité n'affectera pas la note environnementale si l'impact sur la confidentialité (basse) est réglé sur "aucune". Par ailleurs, le fait d'augmenter la condition de confidentialité de "moyenne" à "élevée" ne changera pas la note environnementale lorsque la métrique de l'impact (basse) est réglée sur "complète". En effet, la note secondaire d'impact (partie de la note de base qui calcule l'impact) est déjà réglée à une valeur maximale de 10.

Les valeurs possibles des conditions de sécurité sont récapitulées au Tableau 12. Pour des raisons de commodité, le même tableau est utilisé pour les trois métriques. Plus élevée est la condition de sécurité, plus élevée est la note (il ne faut pas oublier que la note "moyenne" est considérée ont comme note par défaut). Ces métriques modifieront la note dans l'intervalle plus ou moins 2,5.

**Tableau 12 – Evaluation de la note des conditions de sécurité**

Valeur de la métrique	Description
Basse (L)	La perte de [confidentialité intégrité disponibilité] n'a probablement qu'un effet adverse limité sur l'organisation ou les personnes associées à l'organisation (par exemple, employés, clients).
Moyenne (M)	La perte de [confidentialité intégrité disponibilité] a probablement un effet adverse grave sur l'organisation ou les personnes associées à l'organisation (par exemple, employés, clients).
Elevée (H)	La perte de [confidentialité intégrité disponibilité] a probablement un effet adverse catastrophique sur l'organisation ou les personnes associées à l'organisation (par exemple, employés, clients).
Indéfinie (ND)	L'attribution de cette valeur à la métrique n'aura pas d'influence sur la note. C'est un signal adressé à l'équation pour "sauter" cette métrique.

Dans de nombreuses organisations, les ressources TIC sont étiquetées avec des classements de criticité basés sur la localisation du réseau, la fonction commerciale et le risque de perte de revenu ou de vie. Par exemple, l'administration américaine affecte tous ces actifs TIC non classifiés à un groupe d'actifs appelé "Système". Chaque Système doit être associé à trois classements d'impact potentiel pour montrer l'impact potentiel sur l'organisation si le Système est compromis conformément aux trois objectifs de sécurité: confidentialité, intégrité et disponibilité. Ainsi, tout actif TIC non classifié au sein du gouvernement américain a un classement d'impact potentiel faible, modéré ou élevé par rapport aux objectifs de sécurité de confidentialité, intégrité et disponibilité. Ce

système de classement est décrit dans les Federal Information Processing Standards (FIPS) 199. Le CVSS suit ce modèle général du FIPS 199 mais n'exige pas des organisations qu'elles utilisent un système particulier pour attribuer les classements d'impacts faibles, moyens et élevés.

## 6.8 Vecteurs de base, temporels, environnementaux

Chaque métrique du vecteur se compose du nom abrégé de la métrique, suivi par ":" (deux points) puis par la valeur abrégée de la métrique. Le vecteur énumère ces métriques dans un ordre prédéterminé, utilisant le caractère "/" pour séparer les métriques. Si une métrique temporelle ou environnementale ne doit pas être utilisée, on lui donne la valeur "ND" (indéfinie). Les vecteurs de base, temporels et environnementaux sont indiqués ci-après au Tableau 13.

**Tableau 13 – Vecteurs de base, temporels et environnementaux**

Valeur de la métrique	Description
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporel	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environnemental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Par exemple, une vulnérabilité avec des valeurs métriques de base de "Vecteur d'accès: Faible, Complexité d'accès: Moyenne, Authentification: Aucune, Impact sur la confidentialité: aucun, Impact sur l'intégrité: partiel, Impact sur la disponibilité: complet" aurait le vecteur de base suivant: "AV:L/AC:M/Au:N/C:N/I:P/A:C."

## 6.9 Notation – Directives

On trouvera ci-dessous des directives qui devraient aider les analystes à noter les vulnérabilités.

### 6.9.1 Généralités

CONSEIL DE NOTATION N° 1: La notation des vulnérabilités ne devrait pas prendre en compte les interactions avec d'autres vulnérabilités. C'est-à-dire que chaque vulnérabilité doit être notée indépendamment.

CONSEIL DE NOTATION N° 2: Lors de la notation d'une vulnérabilité, il faut considérer l'impact direct sur l'hôte visé simplement. Par exemple, prendre en considération la vulnérabilité d'un script d'un site croisé: l'impact sur un système d'onde utilisateur devrait être nettement supérieur à l'impact sur l'hôte ciblé. Toutefois, il s'agit d'un impact indirect. Les vulnérabilités de script de sites croisés devraient être notées sans impact sur la confidentialité ou la disponibilité et avec un impact partiel sur l'intégrité.

CONSEIL DE NOTATION N° 3: De nombreuses applications, comme les serveurs web, peuvent être exploitées avec des privilèges différents et la notation de l'impact implique de prendre une hypothèse quant aux privilèges utilisés. En conséquence, les vulnérabilités devraient être notées conformément aux privilèges les plus couramment utilisés. Cela peut ne pas refléter nécessairement les meilleures pratiques en matière de sécurité, en particulier pour les applications clients qui sont souvent exploitées avec des privilèges de base. Lorsqu'ils ne sont pas certains des privilèges qui sont les plus courants, les analystes de notation doivent prendre comme hypothèse une configuration par défaut.

CONSEIL DE NOTATION N° 4: Lors de la notation de l'impact d'une vulnérabilité qui peut être exploitée de façons multiples (vecteurs d'attaques), l'analyste doit choisir la méthode d'exploitation qui cause le plus grand impact plutôt que celle qui est la plus courante ou la plus facile à exécuter. Par exemple, si le code d'exploit fonctionnel existe pour une plate-forme mais pas pour une autre, l'exploitabilité doit alors être réglée sur "Fonctionnel". Si deux variantes séparées d'un produit sont dans un stade de développement parallèle (par exemple PHP 4.x et PHP 5.x) et qu'il existe une correction pour une variante mais pas pour une autre, le niveau de correction doit alors être réglé sur "Non disponible".

## **6.9.2 Métrique de base**

### **6.9.2.1 Vecteur d'accès**

CONSEIL DE NOTATION N° 5: 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".

CONSEIL DE NOTATION N° 6: De nombreuses applications clients et utilités présentent des vulnérabilités locales qui peuvent être exploitées à distance soit par des actions avec la complicité de l'utilisateur soit via un traitement automatisé. Par exemple, les utilités de décompression et les scanners de virus analysent automatiquement les courriels entrants. De même, les applications d'aide (suites bureautiques, visionneuses d'images, lecteurs de médias, etc.) sont exploitées lorsque des fichiers malveillants sont échangés par courriels ou sont téléchargés de sites web. Les analystes doivent donc noter le vecteur d'accès de ces vulnérabilités comme "Réseau".

### **6.9.2.2 Authentification**

CONSEIL DE NOTATION N° 7: S'il existe une vulnérabilité dans un système d'authentification proprement dit (par exemple, PAM, Kerberos) ou dans un service anonyme (par exemple, serveurs FTP publics), la métrique doit être notée "Aucune" puisque l'attaquant peut exploiter la vulnérabilité sans fournir de référence valide. La présence d'un compte utilisateur par défaut peut être considérée comme une authentification "Unique" ou "Multiple" (comme approprié), mais il peut avoir une exploitabilité "Elevée" si les références sont rendues publiques.

CONSEIL DE NOTATION N° 8: Il est important de noter que la métrique d'authentification est différente du vecteur d'accès. Ici, les conditions d'authentification sont prises en considération lorsque le système a déjà été accédé. Plus précisément, pour des vulnérabilités exploitables en local, cette métrique ne doit être réglée que sur "Unique" ou "Multiple" si l'authentification est nécessaire au-delà de ce qui est requis pour s'enregistrer dans le système. Un exemple de vulnérabilité exploitable localement qui exige une authentification est une vulnérabilité d'un moteur de base de données à l'écoute sur une prise de domaine Unix (ou une autre interface quelconque non-réseau). Si l'utilisateur doit s'authentifier comme utilisateur de base de données valide pour exploiter la vulnérabilité, cette métrique doit alors être réglée sur "Unique".

### **6.9.2.3 Impacts sur la confidentialité, l'intégrité, la disponibilité**

CONSEIL DE NOTATION N° 9: Les vulnérabilités qui donnent un accès de base devraient être notées avec une perte complète de confidentialité, d'intégrité et de disponibilité alors que celles qui donnent un accès au niveau utilisateur devraient être notées avec seulement une perte partielle de confidentialité, d'intégrité et de disponibilité. Par exemple, une violation d'intégrité qui permet à un attaquant de modifier un fichier de mots de passe d'un système d'exploitation devrait être notée avec un impact complet sur la confidentialité, l'intégrité et la disponibilité.

CONSEIL DE NOTATION N° 10: Les vulnérabilités avec une perte partielle ou complète d'intégrité peuvent également provoquer un impact sur la disponibilité. Par exemple, un attaquant qui peut modifier des dossiers peut probablement les supprimer également.

## 6.10 Equations

Les algorithmes et les équations de notation pour les groupes de métriques de base, temporelles et environnementales sont décrits ci-après. On trouvera à l'adresse [www.first.org/cvss](http://www.first.org/cvss) d'autres discussions sur l'origine et les tests de ces équations. On trouvera à l'Appendice I trois exemples de cas d'utilisation de ces équations.

### 6.10.1 Equation de base

L'équation de base est la fondation de la notation CVSS. L'équation de base (formule version 2.10) est la suivante:

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20*AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise
AccessVector      = case AccessVector of
                    requires local access: 0.395
                    adjacent network accessible: 0.646
                    network accessible: 1.0
AccessComplexity  = case AccessComplexity of
                    high: 0.35
                    medium: 0.61
                    low: 0.71
Authentication    = case Authentication of
                    requires multiple instances of authentication: 0.45
                    requires single instance of authentication: 0.56
                    requires no authentication: 0.704
ConfImpact        = case ConfidentialityImpact of
                    none: 0.000
                    partial: 0.275
                    complete: 0.660
IntegImpact       = case IntegrityImpact of
                    none: 0.000
                    partial: 0.275
                    complete: 0.660
AvailImpact       = case AvailabilityImpact of
                    none: 0.000
                    partial: 0.275
                    complete: 0.660
```

### 6.10.2 Equation temporelle

Si elle est utilisée l'équation temporelle combinera les métriques temporelles à la note de base pour produire une note temporelle allant de 0 à 10. Par ailleurs, la note temporelle produira une note temporelle qui ne sera pas supérieure à la note de base ni à 33% de moins que la note de base. L'équation temporelle est la suivante:

```

TemporalScore = round_to_1_decimal(BaseScore*Exploitability
*RemediationLevel*ReportConfidence)
Exploitability = case Exploitability of
    unproven: 0.85
    proof-of-concept: 0.90
    functional: 0.95
    high: 1.00
    not defined: 1.00

RemediationLevel = case RemediationLevel of
    official-fix: 0.87
    temporary-fix: 0.90
    workaround: 0.95
    unavailable: 1.00
    not defined: 1.00

ReportConfidence = case ReportConfidence of
    unconfirmed: 0.90
    uncorroborated: 0.95
    confirmed: 1.00
    not defined: 1.00

```

**6.10.3 Equation environnementale**

Si on l'utilise, l'équation environnementale combinera les métriques environnementales et la note temporelle pour produire une note environnementale allant de 0 à 10. Par ailleurs, cette équation produira une note qui ne sera pas supérieure à la note temporelle. L'équation environnementale est la suivante:

```

EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)
AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact
sub-equation replaced with the AdjustedImpact equation
AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
*(1-AvailImpact*AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
    none: 0.0
    low: 0.1
    low-medium: 0.3
    medium-high: 0.4
    high: 0.5
    not defined: 0.0

TargetDistribution = case TargetDistribution of
    none: 0.00
    low: 0.25
    medium: 0.75
    high: 1.00
    not defined: 1.00

ConfReq = case ConfReq of
    low: 0.5
    medium: 1.0
    high: 1.51
    not defined: 1.0

IntegReq = case IntegReq of
    low: 0.5
    medium: 1.0
    high: 1.51
    not defined: 1.0

AvailReq = case AvailReq of
    low: 0.5
    medium: 1.0
    high: 1.51
    not defined: 1.0

```

## **7 Ressources additionnelles**

L'Appendice II donne une liste de ressources qui pourra être utile à quiconque implémente le CVSS. Cette liste contient des liens vers des bulletins de vulnérabilité et plusieurs calculateurs CVSS. Les bulletins de vulnérabilité sont utiles lorsque l'on recherche des informations détaillées sur une vulnérabilité particulière. Les calculateurs CVSS sont utiles lorsqu'on essaie de calculer sa propre note de base, temporelle ou environnementale.

## Appendice I

### Exemples d'usage de CVSS

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

On trouvera ci-dessous des exemples d'utilisation de CVSS pour trois vulnérabilités différentes.

#### I.1 CVE-2002-0392

Considérons CVE-2002-0392: Apache Chunked-Encoding Memory Corruption Vulnerability. En juin 2002, une vulnérabilité a été découverte dans les moyens par lesquels le serveur web Apache traite les requêtes codées en utilisant un codage chunk. L'Apache Foundation a expliqué qu'un exploit réussi pouvait conduire à un déni de service dans certains cas et, dans d'autres, à l'exécution d'un code arbitraire avec les privilèges du serveur web.

Puisque la vulnérabilité peut être exploitée à distance, le vecteur d'accès est "Réseau". La complexité de l'accès est "Faible" puisqu'aucune circonstance additionnelle n'est nécessaire pour que cet exploit réussisse; l'attaquant n'a besoin que d'envoyer un message d'exploit correct au dispositif d'écoute web Apache. Aucune authentification n'est demandée pour déclencher la vulnérabilité (tout utilisateur internet peut se connecter au serveur web), aussi, la métrique d'authentification est "Aucune".

La vulnérabilité pouvant être exploitée au moyen de méthodes multiples avec différents résultats, des notes doivent être générées pour chaque méthode et on retient la note la plus élevée.

Si la vulnérabilité est exploitée pour exécuter un code arbitraire avec l'autorisation du serveur web, ce qui modifie le contenu web et, éventuellement, la visualisation des informations de l'utilisateur local ou les informations de configuration (y compris les réglages de connexion et les mots de passe pour les bases de données), les métriques d'impact sur la confidentialité et l'intégrité sont réglées sur "Partiel". Ensemble, ces métriques résultent en une note de base de 6.4.

Si la vulnérabilité est exploitée pour causer un déni de service, l'impact sur la disponibilité est réglé sur "Complet". Ensemble, les métriques donnent une note de base de 7.8. Vu que c'est la note de base la plus élevée possible des options d'exploitation, on l'utilise comme note de base.

Le vecteur de base pour cette vulnérabilité est donc: AV:N/AC:L/Au:N/C:N/I:N/A:C.

On sait que le code d'exploit existe et l'exploitabilité est donc réglée sur "Fonctionnelle". L'Apache Foundation a diffusé des correctifs pour cette vulnérabilité (disponibles pour 1.3 et 2.0) et ainsi, le niveau de remède est "official fix". Naturellement, la confiance du rapport est "Confirmée". Ces métriques ajustent la note de base pour donner une note temporelle de 6.4.

En supposant que la disponibilité est plus importante que d'habitude pour les systèmes visés, et en fonction des valeurs du risque de dommage collatéral et de la distribution de cibles, la note environnementale pourrait varier entre 0.0 ("Aucune", "Aucune") et 9.2 ("Elevée", "Elevée"). Les résultats sont résumés ci-dessous.

```

-----
BASE METRIC                EVALUATION                SCORE
-----
Access Vector              [Network]                (1.00)
Access Complexity          [Low]                    (0.71)
Authentication             [None]                   (0.704)
Confidentiality Impact    [None]                   (0.00)
Integrity Impact          [None]                   (0.00)
Availability Impact       [Complete]               (0.66)
-----
BASE FORMULA                BASE SCORE
-----
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = ((0.6*6.9) + (0.4*10.0) - 1.5)*1.176 == (7.8)
-----
TEMPORAL METRIC           EVALUATION                SCORE
-----
Exploitability             [Functional]             (0.95)
Remediation Level         [Official-Fix]          (0.87)
Report Confidence         [Confirmed]              (1.00)
-----
TEMPORAL FORMULA           TEMPORAL SCORE
-----
round(7.8 * 0.95 * 0.87 * 1.00) == (6.4)
-----
ENVIRONMENTAL METRIC      EVALUATION                SCORE
-----
Collateral Damage Potential [None - High]           {0 - 0.5}
Target Distribution        [None - High]           {0 - 1.0}
Confidentiality Req.      [Medium]                (1.0)
Integrity Req.            [Medium]                (1.0)
Availability Req.         [High]                  (1.51)
-----
ENVIRONMENTAL FORMULA      ENVIRONMENTAL SCORE
-----
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
                    *(1-0.66*1.51)) == (10.0)
AdjustedBase = ((0.6*10)+(0.4*10.0) - 1.5)*1.176 == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0) == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1}) == (0.00 - 9.2)
-----

```

## I.2 CVE-2003-0818

Considérons CVE-2003-0818: Microsoft Windows ASN.1 Library Integer Handling Vulnerability. En Septembre 2003, on a découvert une vulnérabilité qui vise la bibliothèque ASN.1 de tous les systèmes d'exploitation Microsoft. L'exploitation réussie de cette vulnérabilité consiste en un débordement de mémoire permettant à l'attaquant d'exécuter un code arbitraire avec des privilèges administratifs (Système).

Il s'agit d'une vulnérabilité exploitable à distance qui ne nécessite pas d'authentification, le vecteur d'accès est donc "Réseau" et "Authentification" est réglée sur "Aucune". La complexité d'accès est "Faible" puisqu'aucune circonstance d'accès additionnel ou spécialisée n'est nécessaire pour que l'exploit réussisse. Chacune des métriques d'impact est réglée sur "Complet" à cause de la possibilité d'une compromission totale du système. Ensemble, ces métriques résultent en une note de base maximale de 10.0.

Le vecteur de base de cette vulnérabilité est donc: AV:N/AC:L/Au:N/C:C/I:C/A:C.

Il existe des exploits connus de cette vulnérabilité et son exploitabilité est donc "Fonctionnelle". En février 2004, Microsoft a diffusé le correctif MS04-007, correspondant au niveau de correction "Official-Fix" et au rapport de confiance "Confirmé". Ces métriques ajustent la note de base pour donner une note temporelle de 8.3.

En supposant que la disponibilité est moins importante que d'habitude pour les systèmes visés et, en fonction des valeurs du risque de dommage collatéral et de la distribution de cibles, la note environnementale peut varier entre 0.0 ("Aucune", "Aucune") et 9.0 ("Elevée", "Elevée"). Les résultats sont résumés ci-dessous.

BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complexity	[Low]	(0.71)
Authentication	[None]	(0.704)
Confidentiality Impact	[Complete]	(0.66)
Integrity Impact	[Complete]	(0.66)
Availability Impact	[Complete]	(0.66)
FORMULA		BASE SCORE
$\text{Impact} = 10.41 * (1 - (0.34 * 0.34 * 0.34)) == 10.0$ $\text{Exploitability} = 20 * 0.71 * 0.704 * 1 == 10.0$ $f(\text{Impact}) = 1.176$ $\text{BaseScore} = ((0.6 * 10.0) + (0.4 * 10.0) - 1.5) * 1.176 == (10.0)$		
TEMPORAL METRIC	EVALUATION	SCORE
Exploitability	[Functional]	(0.95)
Remediation Level	[Official-Fix]	(0.87)
Report Confidence	[Confirmed]	(1.00)
FORMULA		TEMPORAL SCORE
$\text{round}(10.0 * 0.95 * 0.87 * 1.00) == (8.3)$		
ENVIRONMENTAL METRIC	EVALUATION	SCORE
Collateral Damage Potential	[None - High]	{0 - 0.5}
Target Distribution	[None - High]	{0 - 1.0}
Confidentiality Req.	[Medium]	(1.0)
Integrity Req.	[Medium]	(1.0)
Availability Req.	[Low]	(0.5)
FORMULA		ENVIRONMENTAL SCORE
$\text{AdjustedImpact} = 10.41 * (1 - (1 - 0.66 * 1) * (1 - 0.66 * 1) * (1 - 0.66 * 0.5)) == (9.6)$ $\text{AdjustedBase} = ((0.6 * 9.6) + (0.4 * 10.0) - 1.5) * 1.176 == (9.7)$ $\text{AdjustedTemporal} == (9.7 * 0.95 * 0.87 * 1.0) == (8.0)$ $\text{EnvScore} = \text{round}((8.0 + (10 - 8.0) * \{0 - 0.5\}) * \{0 - 1\}) == (0.00 - 9.0)$		

### I.3 CVE-2003-0062

Considérons CVE-2003-0062: Débordement de mémoire dans NOD32 Antivirus. NOD32 est une application logicielle antivirus développée par Eset. En février 2003, une vulnérabilité par débordement de mémoire a été découverte dans des versions Linux et Unix avant la version 1.013, qui permettait à des utilisateurs locaux d'exécuter un code arbitraire avec les privilèges de l'utilisateur exécutant NOD32. Pour déclencher le débordement de mémoire, l'attaquant doit attendre (ou sur coax) qu'un autre utilisateur (éventuellement un utilisateur de base) analyse un chemin de répertoire d'une longueur excessive.

La vulnérabilité étant exploitable, uniquement pour un utilisateur connecté localement au système, le Vecteur d'accès est "Local". La complexité d'accès est "Elevée" car cette vulnérabilité n'est pas exploitable à la volonté de l'attaquant. Il existe une autre couche de complexité car l'attaquant doit attendre qu'un autre utilisateur utilise le logiciel d'analyse de virus. L'authentification est réglée sur "Aucune" car l'attaquant n'a pas besoin de s'authentifier auprès d'un système additionnel. Si un utilisateur administratif devait utiliser l'analyse de virus, causant ainsi le débordement de la mémoire, une compromission totale du système serait alors possible. Vu que le cas le plus dangereux doit être considéré, chacune des trois métriques d'impact doit être réglée sur "Complet". Ensemble, ces métriques donnent une note de base de 6.2.

Le vecteur de base de cette vulnérabilité est donc: AV:L/AC:H/Au:N/C:C/I:C/A:C.

Le code d'exploit partiel a été divulgué; aussi, la métrique d'exploitabilité est réglée sur "Démonstration de faisabilité". Eset a diffusé un logiciel actualisé, donnant un niveau de correction "official fix" et un rapport de confiance "Confirmé". Ces trois métriques ajustent la note de base pour donner une note temporelle de 4.9.

En supposant que la confidentialité, l'intégrité et la disponibilité revêtent à peu près la même importance pour les systèmes visés et, en fonction des valeurs du risque de dommage collatéral et de la distribution de cibles, la note environnementale pourrait varier entre 0.0 ("aucune", "aucune") et 7,5 ("élevée", "élevée"). Les résultats sont résumés ci-après.

BASE METRIC	EVALUATION	SCORE
Access Vector	[Local]	(0.395)
Access Complexity	[High]	(0.35)
Authentication	[None]	(0.704)
Confidentiality Impact	[Complete]	(0.66)
Integrity Impact	[Complete]	(0.66)
Availability Impact	[Complete]	(0.66)

FORMULA BASE SCORE  
 -----  
 Impact =  $10.41 * (1 - (0.34 * 0.34 * 0.34))$  == 10.0  
 Exploitability =  $20 * 0.35 * 0.704 * 0.395$  == 1.9  
 f(Impact) = 1.176  
 BaseScore =  $((0.6 * 10) + (0.4 * 1.9) - 1.5) * 1.176$  == (6.2)

TEMPORAL METRIC	EVALUATION	SCORE
Exploitability	[Proof-Of-Concept]	(0.90)
Remediation Level	[Official-Fix]	(0.87)
Report Confidence	[Confirmed]	(1.00)

FORMULA TEMPORAL SCORE  
 -----  
 round( $6.2 * 0.90 * 0.87 * 1.00$ ) == (4.9)

ENVIRONMENTAL METRIC	EVALUATION	SCORE
Collateral Damage Potential	[None - High]	{0 - 0.5}
Target Distribution	[None - High]	{0 - 1.0}
Confidentiality Req.	[Medium]	(1.0)
Integrity Req.	[Medium]	(1.0)
Availability Req.	[Medium]	(1.0)

FORMULA ENVIRONMENTAL SCORE  
 -----  
 AdjustedTemporal == 4.9  
 EnvScore = round( $(4.9 + (10 - 4.9) * \{0 - 0.5\}) * \{0 - 1\}$ )  
 == (0.00 - 7.5)

## Appendice II

### Ressources additionnelles

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

On trouvera ci-après une liste de ressources qui pourraient être utiles à quiconque met en œuvre le CVSS. Les bulletins de vulnérabilité sont utiles lorsque l'on recherche des informations détaillées sur une vulnérabilité particulière. Les calculateurs CVSS sont utiles lorsqu'on essaye de calculer sa propre note de base, temporelle ou environnementale.

#### Bulletins de vulnérabilité

- Le NIST (National Institute of Standards and Technology) tient à jour une NVD (National Vulnerability Database), site Internet avec le bulletin de vulnérabilités qui inclut des notes de base CVSS. Le NIST propose ces bulletins sur le web en plus d'informations XML gratuites. On peut les trouver aux adresses: <http://nvd.nist.gov/nvd.cfm>, et <http://nvd.nist.gov/download.cfm#XML>, respectivement.
- IBM Internet Security Systems (ISS) publie gratuitement des bulletins de vulnérabilités X-Force. Ils comprennent des notes de base et temporelles CVSS et sont disponibles à l'adresse: <http://xforce.iss.net/xforce/alerts>.
- Qualys publie des références de vulnérabilité qui incluent à la fois des notes CVSS de base et temporelles. On les trouve à l'adresse: <http://www.qualys.com/research/alerts/>.
- Les bulletins de vulnérabilité Cisco incluant les notes CVSS de base et temporelles sont accessibles à l'adresse: <http://tools.cisco.com/MySDN/Intelligence/home.x>. (NOTE –Nécessite un compte Cisco Connection Online.).
- Tenable Network Security publie des plugins pour l'outil d'analyse de vulnérabilités Nessus. Ces plugins, qui incluent la note CVSS de base, sont disponibles à l'adresse: <http://www.nessus.org/plugins/>.
- JPCERT/CC et IPA tiennent à jour les JVN (Japan Vulnerability Notes), bulletins de vulnérabilités sur le web qui incluent des notes CVSS de base. JVN fournit ces bulletins sur le web en plus d'informations XML gratuites. On peut les trouver aux adresses: <http://jvndb.jvn.jp/en/> et <http://jvndb.jvn.jp/en/apis/>, respectivement.

#### Calculateurs CVSS

- Calculateur NIST CVSSv2:  
<http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>
- Agence d'information et de promotion de la technologie du Japon  
<http://jvndb.jvn.jp/en/cvss/index.html>

## Bibliographie

- [b-1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, *CVSS: A Common Vulnerability Scoring System*, National Infrastructure Advisory Council (NIAC), 2004.
- [b-2] Microsoft Corporation. *Microsoft Security Response Center Security Bulletin Severity Rating System*. Novembre 2002 [cité le 16 mars 2007]. Disponible à l'adresse URL: <http://www.microsoft.com/technet/security/bulletin/rating.mspx>.
- [b-3] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cité le 16 mars 2007]. Disponible à l'adresse URL: <http://www.kb.cert.org/vuls/html/fieldhelp>.
- [b-4] SANS Institute. SANS Critical Vulnerability Analysis Archive. Non daté (cité le 16 mars 2007).
- [b-ITU-T X.1500] Recommendation X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.





## SÉRIES DES RECOMMANDATIONS UIT-T

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