Organisation de Coopération et de Développement Économiques

DSTI/CDEP/SDE(2021)9/FINAL

Non classifié **Français - Or. Anglais**

1er février 2023

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INNOVATION
COMITÉ DE LA POLITIQUE DE L'ÉCONOMIE NUMÉRIQUE

Groupe de travail sur la sécurité dans l'économie numérique

Guide de bonnes pratiques sur la coordination de la gestion des vulnérabilités de sécurité numérique

JT03511452

Avant-propos

Ce document a pour but de fournir aux décideurs de politiques publiques une vue d'ensemble des pratiques de coordination des vulnérabilités de sécurité numérique, tout en évitant le jargon technique et les considérations de détail. Il devrait être lu conjointement avec la Recommandation du Conseil sur le traitement des vulnérabilités de sécurité numérique adoptée en 2022.

Ce document a été approuvé et déclassifié par le Comité des Politiques de l'Économie Numérique (CPEN) lors de sa 86ème session en mai 2022, sur proposition de son Groupe de Travail sur la Sécurité dans l'Économie Numérique (SEN). Sa publication a été préparée par le Secrétariat de l'OCDE.

Ce document a été rédigé par Laurent Bernat, du Secrétariat de l'OCDE, avec les apports précieux des délégués du SEN et du CPEN, ainsi que le soutien et les commentaires d'experts impliqués dans les travaux analytiques de l'OCDE sur les vulnérabilités de sécurité numérique initié en 2020, qui ont conduit à l'élaboration de la Recommandation citée plus haut.

Le *Cadre de l'OCDE sur la sécurité numérique : la cybersécurité au service de la prospérité* fournit une présentation d'ensemble des normes et approches de l'OCDE sur la sécurité numérique, et explique comment le traitement des vulnérabilités se positionne dans ce plus vaste paysage.

On trouvera plus d'information sur les travaux de l'OCDE en matière de sécurité numérique à l'adresse : https://oe.cd/securite.

Table des matières

Introduction

Le présent guide de bonnes pratiques vise à aider à la mise en œuvre de la *Recommandation sur la gestion des vulnérabilités de sécurité numérique* (ci-après dénommé « Recommandation sur les vulnérabilités »).[1]

La gestion des vulnérabilités de sécurité numérique couvre la découverte, le traitement (par les responsables du code), l'administration (par les responsables de systèmes) et la divulgation des vulnérabilités par les chercheurs de vulnérabilités. Le présent document s'intéresse à la coordination de la gestion des vulnérabilités – à savoir aux relations entre les responsables de la gestion des vulnérabilités et les chercheurs de vulnérabilités –, qui représente un volet spécifique de la gestion des vulnérabilités.

Ce guide de bonnes pratiques a pour objet d'aider les décideurs à acquérir une compréhension globale de la coordination concrète des vulnérabilités de sécurité numérique, sans toutefois recourir au jargon technique ni entrer dans des considérations détaillées. Il pourrait également aider les experts techniques en sécurité à communiquer avec les décideurs et les spécialistes non techniques de leur organisation (directeurs, membres du conseil d'administration, services de communication et départements juridiques, etc.). S'il devrait être cohérent avec les normes techniques et autres guides destinés aux experts du domaine, il n'a pas vocation à les remplacer, mais vise au contraire à sensibiliser à leur existence et à la nécessité que les acteurs concernés les utilisent.

C'est pourquoi il reste à un niveau relativement élevé et ne couvre pas tous les aspects de la coordination de la gestion des vulnérabilités. Par exemple, il ne formule pas d'orientations à l'intention des chercheurs de vulnérabilités[2], notamment sur les conditions et les modalités relatives à la divulgation des vulnérabilités au public en cas d'échec de la coordination ; ne donne pas de détails tels que les seuils à partir desquels un chercheur de vulnérabilités devrait considérer que le responsable de la gestion des vulnérabilités ne réagit pas, ou tarde trop à prendre des mesures d'atténuation ; n'indique pas comment publier les politiques de divulgation des vulnérabilités ; ne précise pas comment déterminer quelles informations devraient être divulguées au public ; ne fournit pas de détails sur la coordination multipartite ou multi-« fournisseurs » de la gestion des vulnérabilités, etc.

Ces aspects importants, comme de nombreux autres abordés dans les travaux d'analyse de l'OCDE[3], soulèvent des questions complexes qui méritent d'être étudiées plus avant par les parties prenantes avant d'être intégrées dans un document destiné en premier lieu aux décideurs. Le Comité de la politique de l'économie numérique et son Groupe de Travail sur la Sécurité dans l'Économie Numérique pourraient toutefois réviser à l'avenir le présent document afin de tenir compte des progrès réalisés dans ce domaine et de continuer d'informer au mieux les décideurs.

---

1 OCDE (2022), *Recommandation du Conseil sur le traitement des vulnérabilités de sécurité numérique*, OCDE/LEGAL/0482, OCDE, Paris.

2 La Recommandation sur les vulnérabilités préconise que les Adhérents coopèrent avec l'ensemble des parties prenantes au niveau international en vue d'élaborer de telles orientations. Voir IX.2.e.

3 OCDE (2021), "Encouraging vulnerability treatment: Overview for policy makers", *OECD Digital Economy Papers*, No. 307, OECD Publishing, Paris, https://doi.org/10.1787/0e2615ba-en. Voir également la note de synthèse sur ce sujet : www.oecd.org/fr/numerique/encourager-le-traitement-des-vulnerabilites.pdf.

L'absence d'exhaustivité de ce guide de bonnes pratiques devrait pousser les décideurs et l'ensemble des parties prenantes à poursuivre leur dialogue et compléter les parties manquantes.

Le guide de bonnes pratiques s'appuie sur différents guides et documents traitant de la divulgation coordonnée des vulnérabilités cités dans la section Références.

L'Encadré 1 fournit les définitions des termes principaux inclus dans ce document.

Encadré 1. Terminologie

- Les **vulnérabilités de sécurité numérique**, ou « vulnérabilités », s'entendent des faiblesses techniques présentes dans les produits et les systèmes d'information, susceptibles d'être exploitées pour porter préjudice aux activités économiques et sociales. Elles comprennent :
  - les *vulnérabilités de code*, présentes dans le code des produits ; et
  - les *vulnérabilités de système*, qui sont propres aux systèmes d'information et découlent en premier lieu d'erreurs de configuration et de la non-application des mises à jour de sécurité, des correctifs ou d'autres mesures d'atténuation.
- Les **chercheurs de vulnérabilités** désignent les personnes ou les organisations qui détectent les éventuelles vulnérabilités de code ou de système et agissent dans l'intention de réduire le risque de sécurité connexe. Ils sont parfois dénommés « pirates éthiques » ou « chapeaux blancs ».
- Les **responsables des vulnérabilités** désignent les parties prenantes chargées d'atténuer les vulnérabilités dont ils ont connaissance. Il peut s'agir des **responsables du code** (également dénommés « prestataires »), qui sont chargés de développer une couche de code intégrée à un produit et d'en assurer la maintenance, y compris de traiter les vulnérabilités (par exemple en concevant un correctif et en le diffusant, notamment par le biais d'une mise à jour de sécurité). Les responsables du code forment la première ligne de défense contre les acteurs malveillants. Ils sont souvent appelés prestataires, fournisseurs, développeurs, chargés de maintenance ou fabricants. Les responsables des vulnérabilités incluent également les **responsables des systèmes**, qui sont chargés de corriger les vulnérabilités de système, notamment par le biais de l'administration des vulnérabilités (par exemple en appliquant les correctifs et les mises à jour de sécurité). Ils forment la deuxième ligne de défense. La conjugaison de ces deux lignes de défense contribue à réduire le risque de sécurité découlant de l'exploitation éventuelle des vulnérabilités.
- Le **traitement des vulnérabilités** désigne les processus fondés sur le risque mis en œuvre par les responsables de code pour vérifier les informations relatives à une vulnérabilité qui vient d'être découverte et la corriger en élaborant les mesures d'atténuation appropriées et en les diffusant auprès des responsables de système concernés (mise à jour de sécurité, correctif, solution de contournement, etc.).
- L'**administration des vulnérabilités** désigne les processus continus, fondés sur le risque, permettant à un responsable de système de savoir si son écosystème numérique présente des vulnérabilités et de prendre des décisions et des mesures de gestion du risque appropriées pour les atténuer.
- Les **rapporteurs de vulnérabilités** désignent les personnes ou les organisations qui signalent des vulnérabilités. Parfois appelés « découvreurs », ils incluent les chercheurs de vulnérabilités et d'autres acteurs tels que les coordinateurs, les utilisateurs des produits ou des systèmes d'information, les personnes chargées de réaliser les tests d'intrusion, etc.

- La **gestion des vulnérabilités** s'entend du processus général englobant la découverte, le traitement (par les responsables de code), l'administration (par les responsables de système) et la divulgation des vulnérabilités. Elle couvre toutes les actions entreprises pour découvrir les vulnérabilités et :
  - *pour les vulnérabilités de code*, concevoir une mesure d'atténuation (de type correctif, mise à jour de sécurité, solution de contournement), la diffuser auprès des utilisateurs des produits concernés et divulguer les vulnérabilités au public ou à la communauté des acteurs de la sécurité ; et
  - *pour les vulnérabilités de système*, appliquer une mesure d'atténuation existante ou corriger l'erreur de configuration.
- La **divulgation coordonnée des vulnérabilités** (DCV) désigne le processus par lequel les responsables des vulnérabilités et les chercheurs de vulnérabilités coopèrent dans le but de trouver des solutions pour réduire le risque découlant d'une vulnérabilité. La DCV fait partie de la gestion des vulnérabilités.

Source : *Recommandation du Conseil sur le Traitement des Vulnérabilités de Sécurité Numérique*.

I.Partager une identité de vues

1. Toutes les parties prenantes partagent une identité de vues sur les points fondamentaux suivants :

   a. Tous les produits intégrant du code peuvent présenter des vulnérabilités ; tous les produits peuvent sembler exempts de vulnérabilités à un certain point ou dans un contexte donné, mais devenir vulnérables à un stade ultérieur ou lorsque le contexte évolue ; tous les systèmes d'information peuvent présenter des vulnérabilités liées à des défauts de configuration et à la non-application des correctifs et des mises à jour de sécurité des produits.

   b. Ces vulnérabilités peuvent représenter un danger car des acteurs malveillants peuvent les exploiter et causer des dommages à toutes les parties prenantes, voire, dans certains cas, à l'économie et à la société dans leur ensemble. Les attaques de sécurité numérique mettent à mal la prospérité économique et sociale et les droits humains, sapent la confiance dans l'économie numérique, réduisent les avantages potentiels de la transformation numérique, et menacent la sécurité, y compris celle des individus, la vie privée, ainsi que l'exécution des activités essentielles au fonctionnement des économies et des sociétés, telles la santé, le traitement de l'eau, la distribution d'énergie et les élections.

   c. Si toutes les vulnérabilités ne peuvent être éliminées, il est néanmoins possible de corriger, ou au moins de limiter nombre d'entre elles, et la priorité devrait être accordée à celles qui posent les risques les plus élevés.

   d. La divulgation coordonnée des vulnérabilités (DCV) est un processus par lequel les parties prenantes responsables de l'élimination des vulnérabilités dans les produits ou les systèmes (responsables des vulnérabilités) et les chercheurs de vulnérabilités qui ont détecté une vulnérabilité dans lesdits produits ou systèmes allient leurs efforts et travaillent de concert dans un but commun : renforcer la sécurité de l'ensemble des parties prenantes (ou réduire le risque de sécurité numérique auquel elles sont confrontées). L'un des principaux objectifs de la DCV est de réduire

l'avantage des adversaires le temps de corriger une vulnérabilité. Il s'agit là d'une composante importante de la gestion des vulnérabilités.

e. Il n'existe pas de solution unique pour signaler et divulguer une vulnérabilité. Les parties prenantes conviennent de mettre en œuvre des bonnes pratiques et des politiques tout en sachant qu'elles proposent une marche à suivre applicable à des cas généraux qui n'est pas nécessairement optimale dans toutes les situations. C'est pourquoi elles coopèrent à la fois pour gérer chaque situation dans le respect des bonnes pratiques et pour déterminer la meilleure approche lorsque ces dernières n'offrent pas une solution optimale pour réduire le risque dans des cas particuliers.

f. L'efficacité de la divulgation des vulnérabilités est autant une question de confiance entre des personnes qu'un défi technique.

II.Assumer ses responsabilités

2. Les responsables de vulnérabilités et les chercheurs de vulnérabilités travaillent de concert pour gérer les vulnérabilités et partager les informations avec les autres parties prenantes. Ils ont pour objectif commun de minimiser la fenêtre d'exposition de ces dernières à l'exploitation des vulnérabilités par des acteurs malveillants. Si le temps est généralement un facteur crucial, les parties prenantes coopèrent pour s'assurer que les mesures de remédiation ou d'atténuation sont soumises à des tests suffisants avant d'être diffusées, de manière à réduire au maximum le risque de créer de nouvelles vulnérabilités et d'autres effets secondaires néfastes.

II.1 Responsables de la gestion des vulnérabilités

3. Les responsables de vulnérabilités :

   a. Sont chargés d'assurer la sécurité du système qu'ils exploitent ou du produit qu'ils ont conçu, et de gérer les vulnérabilités que ce système ou produit présente en fonction du risque qu'elles font peser sur eux-mêmes, les utilisateurs, des tierces parties, et l'économie et la société au sens large ;

   b. Sont préparés à recevoir et traiter des signalements de vulnérabilités sollicités et non sollicités dans le cadre de leur devoir de diligence et responsabilité normaux, et à coordonner la divulgation des vulnérabilités selon leurs possibilités (taille, ressources, nombre de signalements, etc.) ;

   c. Publient et mettent en œuvre une politique de divulgation des vulnérabilités (PDV) (voir ci-après, section IV) ;

   d. Traitent l'ensemble des signalements de vulnérabilités avec une attention et un respect équivalents, fournissent un retour d'informations circonstancié et proactif au chercheur de vulnérabilités sur la reproduction, la remédiation ou l'atténuation, et la divulgation de la vulnérabilité ; reconnaissent et, dans la mesure du possible, mettent en valeur publiquement le travail du chercheur de vulnérabilités (dans un communiqué de presse, un bulletin de sécurité et les avis de vulnérabilités) ; apportent leur appui aux chercheurs de vulnérabilités s'ils sont visés par une procédure judiciaire injustifiée.

4. Plus précisément :

   a. *Les responsables du code* :

- Traitent toute vulnérabilité connue dans le cadre des tâches de support de base de leurs produits et du cycle de développement sécurisé des produits ;
- Éclairent et coordonnent les efforts de remédiation avec les acteurs amont et aval lorsque la vulnérabilité du code est intégrée à des produits tiers (coordination multipartite ou au niveau de la chaîne d'approvisionnement, par exemple).

b. Les *responsables de système* mettent en place des cycles de gestion systématique des vulnérabilités afin :

- de détecter les erreurs de configuration et de s'assurer qu'elles sont rapidement corrigées ;
- d'identifier quels produits, parmi ceux qu'ils utilisent, présentent des vulnérabilités connues et de s'assurer que les dernières mises à jour de sécurité et autres mesures de remédiation ou d'atténuation (correctifs, solutions de contournement, par exemple) sont appliquées dans les plus brefs délais, en tenant compte du risque opérationnel et technique inhérent à la gestion des vulnérabilités.

II.2 Chercheurs de vulnérabilités

5. Les chercheurs de vulnérabilités sont responsables de leurs actions, notamment de la façon dont ils découvrent, signalent et divulguent les vulnérabilités. Ils s'en tiennent à ce qu'il est nécessaire de faire pour démontrer l'existence d'une vulnérabilité ou les moyens de l'atténuer.

6. Les chercheurs de vulnérabilités :

a. Signalent la vulnérabilité au responsable de la vulnérabilité en premier lieu et dès que possible après l'avoir découverte, ou contactent un coordinateur (voir ci-après, la section IV) s'ils ne peuvent joindre le responsable de la gestion, en utilisant dans tous les cas des moyens de communication suffisamment sûrs ;

b. Fournissent des documents et matériels clairs pour appuyer le processus de reproduction permettant au responsable des vulnérabilités de vérifier que la vulnérabilité existe et de comprendre comment un acteur malveillant pourrait l'exploiter ;

c. Lisent les conditions définies par les responsables de la gestion des vulnérabilités dans leur PDV, s'efforcent de les suivre et, en cas de désaccord sur les conditions ou en l'absence de PDV, contactent un coordinateur et mettent en œuvre les bonnes pratiques en matière de DCV ;

d. Laissent au responsable de la gestion des vulnérabilités un délai raisonnable pour traiter le signalement de vulnérabilité ;

e. Ne conditionnent pas le signalement d'une vulnérabilité à l'obtention d'une récompense. La décision d'octroyer une récompense revient au responsable des vulnérabilités.

III.Instaurer une confiance durable

7. Toutes les parties à la DCV instaurent et maintiennent la confiance, notamment en observant les principes suivants :

a. **Présumer que les autres parties prenantes font preuve de bienveillance,** de bonnes intentions et de bonne volonté.

b. **Communiquer** clairement **ses intentions** et s'efforcer, en toute bonne foi, de comprendre les attentes et points de vue respectifs.

c. Maintenir une **communication permanente ou fréquente** empreinte de qualité, de respect mutuel, de patience et de transparence.

d. **Gérer** de manière adéquate **les informations sensibles** et utiliser des canaux de communication suffisamment sécurisés.

e. Faire preuve de **transparence** sur les processus et les étapes (délais) attendus, notamment pour ce qui est des processus de remédiation et de divulgation.

f. **Réduire l'incertitude**, la surprise et le risque de mécontentement des autres parties à la DCV.

g. **Négocier les attentes** et les délais si les processus standard ne sont pas adaptés.

h. **Éviter les pressions ou menaces de recours juridique ou de mesure coercitive**, réelles ou perçues, ainsi que les mesures d'escalade, y compris les actions judiciaires, dans la mesure du possible, afin d'éviter les effets dissuasifs sur la recherche de vulnérabilités attendue.

IV.Faire appel à un coordinateur

8. Les parties prenantes qui peinent à mettre en place ou à mener à bien un processus de DCV font appel à un coordinateur tiers de confiance. Le rôle de coordinateur est souvent assuré par une équipe de réponse aux incidents de sécurité informatique (CSIRT) ou une équipe de réponse aux incidents de sécurité des produits (PSIRT).

9. Un coordinateur peut par exemple aider à mettre en relation les parties prenantes, fournir une analyse technique complémentaire et d'autres formes d'appui, en particulier en cas de désaccord entre les parties ou de mécontentement de l'une d'elles, ou pour les signalements complexes tels que ceux impliquant plusieurs responsables des vulnérabilités (coordination multipartite ou au niveau de la chaîne d'approvisionnement). Le coordinateur peut aussi aider à résoudre les difficultés rencontrées à l'échelle internationale. Par ailleurs, certains coordinateurs peuvent aider au partage de connaissances sur les vulnérabilités au sein de la communauté des experts techniques en sécurité, en publiant par exemple des avis de sécurité.

V. Adopter une politique de divulgation des vulnérabilités

10. Une PDV devrait à tout le moins mentionner un point de contact auquel les chercheurs de vulnérabilités peuvent adresser les signalements de vulnérabilités en toute sécurité.

11. Une PDV repose sur les principes suivants :

a. **Clarté** : une PDV est publique, utilise des termes simples, faciles à comprendre, sans jargon ni formulation ambiguë. Elle n'est pas modifiée fréquemment et, le cas échéant, les changements apportés font l'objet d'un suivi, sont expliqués et documentés.

b. **Portée** : une PDV reflète l'intention de l'organisation avec fidélité, clarté et précision ; elle expose le périmètre du programme de divulgation des vulnérabilités,

qui est proportionné aux capacités du responsable des vulnérabilités de manière à traiter efficacement les signalements.

c. **Règles du jeu** : une PDV décrit les pratiques autorisées et interdites ; expose les conséquences du respect et du non-respect de ses dispositions, y compris la protection juridique offerte aux chercheurs de vulnérabilités qui s'y conforment ; définit les conditions dans lesquelles le responsable de la gestion des vulnérabilités convient de ne pas intenter ou appuyer une action en justice contre les chercheurs de vulnérabilités ; et encourage les participants à demander des précisions à l'organisation avant de se livrer à des pratiques qui pourraient contrevenir aux dispositions de la politique ou que cette dernière ne couvrirait pas.

d. **Transparence** : une PDV expose les modalités du traitement des vulnérabilités signalées, indique clairement les conditions de communication sécurisée et éventuellement anonyme, précise les possibilités de reconnaissance et de récompense (le cas échéant), la chronologie, les délais de réponse et les communications de suivi pendant le processus, la confidentialité, et, pour les vulnérabilités affectant le code : les attentes quant à la mise au point d'une solution, sa diffusion et la divulgation au public.

e. **Facilitation** : une PDV mentionne la possibilité de faire appel à un coordinateur pour faciliter le processus.

VI. Mettre en place des processus internes appropriés pour la divulgation coordonnée des vulnérabilités

12. Les responsables des vulnérabilités abordent la DCV comme un complément et non comme un substitut aux autres mesures de sécurité.

13. Lorsqu'ils recourent à la divulgation coordonnée des vulnérabilités, les responsables des vulnérabilités :

a. **Affectent des ressources internes suffisantes**, définissent clairement les rôles et responsabilités quant à l'exécution des tâches d'analyse et de communication des vulnérabilités, et déploient progressivement leur programme de divulgation des vulnérabilités, selon leur courbe d'apprentissage, leur maturité et leurs capacités internes de traitement des signalements. Pour ce faire, ils peuvent s'appuyer sur des indicateurs tels que les vulnérabilités signalées, les faux-positifs, les délais de communication avec les chercheurs, et les délais quant à l'atténuation des vulnérabilités détectées ;

b. **Mettent en place une coordination interne** avec les équipes opérationnelles, juridiques et de communication, et intègrent la DCV aux processus décisionnels plutôt que d'en faire un processus technique isolé ;

c. **Mettent en place un socle solide de processus et de relations éprouvés**, conformes aux normes, aux documents d'orientation et aux meilleures pratiques à l'échelle internationale, afin de garantir une réponse et des relations prévisibles avec les chercheurs de vulnérabilités et les tierces parties, de mettre en œuvre un mécanisme de prise en charge clair, publié, correctement sécurisé et faisant l'objet d'une surveillance régulière, et de prévoir des canaux appropriés pour la communication avec les chercheurs de vulnérabilités ;

d. **Tiennent compte des intérêts des tierces parties**. Par exemple, si la vulnérabilité signalée concerne un composant tiers d'un produit, le fabricant dudit produit étend le processus de DCV au responsable du code du composant ;

e. **Se conforment aux normes techniques internationales**, le cas échéant, par exemple pour ce qui est de la représentation et de l'échange des informations relatives aux vulnérabilités, de manière à faciliter l'utilisation d'outils automatisés par les tierces parties ;

f. **Anticipent les difficultés**, par exemple en décidant, avant le lancement du programme de DCV, de la façon de traiter les violations accidentelles de la PDV, sans volonté de nuire, et les violations intentionnelles et malveillantes ;

g. **Mettent en place un cycle d'amélioration**, en tirant les enseignements des signalements de vulnérabilités afin d'œuvrer à l'amélioration des pratiques générales en matière de sécurité, y compris du processus de DCV lui-même.

Références

L'aperçu des bonnes pratiques exposé ci-dessus s'appuie sur une analyse des documents suivants (cités dans l'ordre chronologique) et sur les contributions des délégations et des experts auprès de l'OCDE:

1. Christey Steve, Wysopal Chris (2002), *Responsible Vulnerability Disclosure Process*.
2. US-CERT (2012), *Common Industrial Control System Vulnerability Disclosure Framework*.
3. ENISA (2016), *Good Practice Guide on Vulnerability Disclosure*. *From challenges to recommendations.*
4. Rabobank, CIO Platform Nederland (2016), *Manifesto on Co-ordinated Responsibility Disclosure*.
5. NTIA Safety Working Group (2016), *« Early Stage » Co-ordinated Vulnerability Disclosure Template*, version 1.1.
6. Householder D., G. Wassermann, A. Manion, C. King (2017), *The CERT® Guide to Co-ordinated Vulnerability Disclosure*, CMU/SEI-2017-SR-022.
7. FIRST (2017), *Guidelines and Practices for Multi-Party Vulnerability Co-ordination and Disclosure*, v 1.0.
8. US Department of Justice (2017), *A Framework for a Vulnerability Disclosure Program for Online Systems, version 1.0*.
9. Dutch National Cyber Security Centre (2018), *Co-ordinated Vulnerability Disclosure: The Guideline*.
10. Cybersecurity Coalition (2019), *Policy Priorities for Co-ordinated Vulnerability Disclosure and Handling*.
11. Center for Cybersecurity Policy and Law (2019), *Improving Hardware Component Vulnerability Disclosure*.
12. Business Software Alliance (BSA) (2019), *Guiding Principles for Co-ordinated Vulnerability Disclosure*.
13. UK National Cybersecurity Center (NCSC-UK) (2020), *Vulnerability Disclosure Toolkit*.
14. Cybersecurity and Infrastructure Security Agency (CISA) (2020), *Binding Operational Directive 20-01*. *Develop and Publish a Vulnerability Disclosure Policy*.