Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

OFCS – GESTION DES VULNÉRABILITÉS

Divulgation des vulnérabilités

Guide à l'usage des organisations et des entreprises

01.02.2024

Table des matières

1 Introduction

Au cas où une personne interne ou externe découvrirait une faille informatique dans les systèmes ou produits de votre organisation ou entreprise, il faudrait qu'elle puisse la signaler aussitôt au service informatique compétent dans votre entreprise ou organisation, selon un processus clairement défini.

Une procédure d'annonce claire et compréhensible doit permettre aux organisations et entreprises de toute taille d'obtenir directement des informations sur les vulnérabilités, et donc de les corriger d'autant plus rapidement et de manière plus ciblée. Une procédure clairement définie montre encore que l'organisation ou l'entreprise prend au sérieux le thème de la sécurité et qu'elle s'efforce d'améliorer en permanence ses systèmes et ses produits.

Le présent guide de l'OFCS sur la divulgation des vulnérabilités (*vulnerability disclosure*) s'adresse aux organisations et aux entreprises. Il vise à les aider à réaliser à l'interne une procédure d'annonce à cet égard. Cette procédure comprend les trois grands volets suivants: communication; lignes directrices; et security.txt.

Le guide repose essentiellement sur la norme internationale de divulgation des vulnérabilités (ISO/IEC 29147:2018). Il définit les techniques utilisables et les lignes directrices à suivre pour la réception des annonces de vulnérabilités et la publication des informations destinées à les corriger. La norme ISO/IEC 29147:2018 a été adoptée le 3 mai 2020 par le Comité européen de normalisation (CEN).

1.1. Objectifs de la divulgation des vulnérabilités

La divulgation des vulnérabilités permet, d'une part, de corriger les failles existantes et, d'autre part, de prendre des décisions mieux informées face aux risques. Selon la norme ISO/IEC 29147:2018, la divulgation des vulnérabilités poursuit plusieurs objectifs prioritaires:

- réduire les risques en corrigeant les vulnérabilités et en informant les utilisateurs;
- limiter autant que possible le préjudice et les coûts;
- fournir aux utilisateurs des informations suffisantes pour leur permettre d'évaluer les risques dus aux vulnérabilités;
- définir les attentes des parties prenantes pour faciliter l'interaction et la coordination entre elles.

2 Structure du guide

Le présent guide comporte trois grands volets qui jouent chacun un rôle essentiel dans le processus de divulgation des vulnérabilités:

2.1 Communication

2.1.1 Mise à disposition de coordonnées spécifiques

Une communication rapide et sans détours s'avère décisive pour tous les protagonistes.
Si des collaborateurs de votre organisation ou entreprise, des chercheurs en sécurité, des pirates éthiques, l'OFCS voire le grand public ont connaissance d'une vulnérabilité technique de votre organisation ou entreprise, il est important que tous ces acteurs puissent rapidement trouver et contacter le service informatique responsable de corriger cette vulnérabilité.

Or bien souvent, ces coordonnées spécifiques manquent. Le site Internet n'indique fréquemment qu'un numéro de téléphone central ou une adresse électronique générale. Par conséquent, l'auteur de l'annonce doit réexpliquer plusieurs fois le problème avant de tomber sur la bonne personne, ce qui fait perdre un temps précieux. Il est potentiellement déjà trop tard quand l'information parvient au responsable. Souvent aussi, de telles informations sont ignorées au lieu d'être transmises, et donc le service compétent n'a pas connaissance de la vulnérabilité. C'est à la fois frustrant pour les lanceurs d'alerte et irritant pour l'organisation ou l'entreprise, qui perd autant d'occasions d'améliorer sa propre cybersécurité.

Pour remédier à ce problème, les coordonnées des responsables informatiques doivent être aisées à trouver, ou du moins un processus de signalement des vulnérabilités doit être défini dans l'entreprise. L'OFCS recommande d'indiquer les coordonnées dans la rubrique «Contact» du site Internet. Il faudrait également indiquer les options de contact dans un fichier «security.txt» conçu à cet effet et disponible sur le site (voir point 2.3 «security.txt»).

2.1.2 Exigences techniques

Une adresse électronique créée à cet effet ou un formulaire Web permettent de garantir que toute information concernant une vulnérabilité parvienne au bon endroit dans votre organisation ou entreprise.

Si la procédure d'annonce utilisée est basée sur le Web (par ex. formulaire Web), il faut veiller à ce que le transfert des données soit chiffré, par exemple en utilisant le protocole TLS (HTTPS). De même, la communication par courriel devrait recourir à des solutions de chiffrement et de signature comme S/MIME ou PGP. Les clés publiques nécessaires doivent être accessibles sur le site internet.

Un exemple de formulaire Web figure sur le site Internet de l'OFCS:

https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html

2.1.3 Processus

Le présent guide définit les quatre étapes du processus de traitement des vulnérabilités:

Réception de l'annonce :
Si vous recevez une annonce portant sur une possible vulnérabilité, vous devriez autant que possible en accuser réception sur-le-champ, mais au plus tard dans les sept jours ouvrables, en remerciant l'auteur de la découverte. La réponse pourra être générée automatiquement, mais devrait être pertinente. Il faudrait qu'elle comporte un numéro de suivi ou un identifiant et qu'elle donne des informations provisoires sur l'état du dossier.

Vérification :
Il s'agit dans un second temps de contrôler et de vérifier la vulnérabilité annoncée. En cas d'afflux d'un nombre élevé d'annonces, un tri doit être effectué sur la base de l'évaluation individuelle des risques pour chaque vulnérabilité reçue. À l'issue de cet examen, nous vous recommandons d'informer l'auteur de l'annonce du résultat de cette première évaluation.

Correction de la vulnérabilité :
Tandis que le processus de traitement des vulnérabilités suit son cours, vous devriez régulièrement communiquer avec l'auteur de l'annonce. Une telle communication devrait contenir les informations suivantes:

- actualisation du statut;
- nouvelles informations pertinentes;
- modifications apportées aux projets existants;
- calendrier de publication.

Publication :
La communication est le facteur clé. Des coordonnées faciles à trouver ainsi qu'une communication prompte, transparente et empreinte de respect tout au long du processus de traitement des vulnérabilités soutiennent l'engagement et la motivation des auteurs d'annonces.

2.2 Lignes directrices

Des lignes directrices claires vous permettent de préciser, d'une part, ce que vous attendez d'une personne qui vous annonce une vulnérabilité et, d'autre part, ce qu'une telle personne est en droit d'attendre de votre organisation ou entreprise. Les déclarants peuvent ainsi collaborer avec vous dans un cadre préalablement convenu.

Selon la norme ISO/IEC 29147:2018, les lignes directrices relatives à la publication des vulnérabilités doivent obligatoirement aborder certains points, alors que d'autres sont seulement recommandés:

- procédure de prise de contact, par exemple lien/courriel ou formulaire Web **(obligatoire)**;
- informations à mentionner dans le rapport sur la vulnérabilité; voir aussi ISO/IEC 29147:2018, annexe B **(recommandé)**;
- exigences relatives à la communication **(recommandé)**;
- remerciements **(recommandé)**;
- aspects juridiques **(recommandé)**.

Vous trouverez un exemple de lignes directrices sur le site Internet de l'OFCS:
https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html

D'autres exemples se trouvent dans la norme ISO/IEC 29147:2018, annexe A.

2.3 security.txt

La norme «security.txt» permet de savoir rapidement à qui s'adresser, dans une organisation ou entreprise, pour toute question liée à la sécurité. Elle exige d'enregistrer, dans le répertoire «/.well-known» préalablement défini sur le serveur Web qui héberge le site Internet, un fichier texte intitulé «security.txt». Ce fichier renfermera au minimum les coordonnées des responsables de la sécurité du site Internet ou de l'organisation ou entreprise. Il est possible d'ajouter au même emplacement des liens conduisant à des clés de chiffrement, à des directives sur la sécurité et à des programmes spéciaux de divulgation des vulnérabilités ou de primes aux bogues (*bug bounty*).

Cette norme a été officiellement reconnue en avril 2022 sous le titre «RFC 9116». Toujours plus d'entreprises technologiques et d'organisations gouvernementales du monde entier l'appliquent désormais sur Internet.

Le fichier «security.txt» comprendra des indications obligatoires et d'autres optionnelles:

Quoi	Description	Obligatoire	Optionnel
Contact	Lien vers un formulaire web ou adresse électronique permettant de contacter l'organisation ou l'entreprise pour toute question liée à la sécurité. Veillez à ajouter le préfixe «https://» ou «mailto:» devant chaque URL.	X	
Date d'expiration	Date et heure où il faudra considérer le contenu du fichier «security.txt» comme périmé. Veillez à actualiser régulièrement cette valeur et à réexaminer constamment votre fichier.	X	
Langue préférée	Liste des langues, séparées par des virgules, que parle votre service informatique. Vous pouvez indiquer plusieurs langues.		X
Options de chiffrement	Lien vers une clé (par ex. PGP ou S/MIME) dont les chercheurs en sécurité pourront se servir pour communiquer en toute sécurité avec vous.		X
Remerciements	Lien vers une page Internet où l'organisation / l'entreprise remercie les chercheurs en sécurité qui ont signalé un problème de sécurité et qui souhaitent être mentionnés à ce titre. N'oubliez pas le préfixe «https://».		X
Lien vers le fichier security.txt	Adresse URL de votre fichier security.txt. Il est important de l'indiquer si votre fichier security.txt est muni d'une signature numérique, car ainsi l'emplacement du fichier security.txt pourra lui aussi avoir sa propre signature numérique.		X
Politique de sécurité	Lien vers une directive précisant comment les chercheurs en sécurité devraient procéder pour vous signaler des problèmes de sécurité. Pensez à indiquer le préfixe «https://».		X
Offres d'emploi	Lien vers toutes les offres d'emploi liées à la sécurité dans votre entreprise. Veillez à inclure le préfixe «https://».		X

Cette liste n’est pas exhaustive. Pour plus d’informations, veuillez consulter la norme RFC9116 (voir annexe).

2.2.1 Exemple de fichier «security.txt» (site Internet de l’OFCS)

https://www.ncsc.admin.ch/.well-known/security.txt

```
# In the event that you have discovered a technical vulnerability in an IT system of the federal government,
# we encourage you to report it to the National Cyber Security Centre NCSC using the Coordinated Vulnerability
Disclosure program.
# We forward your request to the appropriate unit.
# If you are interested in participating in the NCSC bug bounty programs you can apply here:
https://www.bugbounty.ch/ncsc

Contact: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-
melden.html
Contact: mailto:incidents@ncsc.ch
Expires: 2024-12-31T23:59:59.000Z
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/pgp_ncsc_incidents.asc.download.asc/NCSC_Incidents.asc
Encryption: https://www.ncsc.admin.ch/dam/ncsc/de/Key/smime_incidents_ncsc_ch_22.cer.download.cer/
smime_incidents_ncsc_ch_22.cer
Preferred-Languages: en, de, fr, it
Canonical: https://www.ncsc.admin.ch/.well-known/security.txt
Policy: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-
melden/scope-and-rules.html
```

3 Liens utiles

ISO/IEC 29147:2018 Standard: Divulgation de vulnérabilité
https://www.iso.org/fr/standard/72311.html

ENISA - Coordinated Vulnerability Disclosure policies in the EU
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

IETF - RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure
https://www.ietf.org/rfc/rfc9116.pdf

OSCE learning: cyber/ICT security CBM 16: Coordinated Vulnerability Disclosure
https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about

OFCS - Actuel: de prétendus chercheurs en cybersécurité réclament des primes
https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/wochenrueckblick_38.html