Procédure

Politique de divulgation coordonnée des vulnérabilités

Sécurité de l'information

Informations générales

Numéro de document :	POL-MGT-019
Version :	1
Date de publication :	27/07/2026
Classification :	Public

1 Politique de divulgation coordonnée des vulnérabilités

1.1 Pourquoi cette politique

La sécurité de ses informations et de ses systèmes constitue une priorité essentielle pour la CILE. Malgré l'attention constante que nous portons à leur protection, il est possible que certaines vulnérabilités subsistent.

Si vous découvrez une vulnérabilité dans l'un de nos systèmes, nous vous invitons à nous en informer afin que les mesures nécessaires puissent être prises dans les meilleurs délais. La CILE souhaite collaborer avec vous dans une démarche responsable, afin de renforcer la protection de ses systèmes d'information.

La présente politique de divulgation s'applique à l'ensemble des systèmes d'information de la CILE. Pour toute question, vous pouvez nous contacter à l'adresse suivante : vulnerabilite@cile.be.

1.2 Principe de coopération

Si vous découvrez une vulnérabilité dans l'un de nos systèmes, veuillez s'il vous plait :

- Signaler la vulnérabilité dès que possible après sa découverte : Demander un lien sécurisé via vulnerabilite@cile.be (Ne pas envoyer d'information confidentielle via email, afin d'éviter que les informations ne tombent entre de mauvaises mains).
- Fournir suffisamment d'informations pour reproduire la vulnérabilité, afin que le problème soit résolu le plus rapidement possible. En règle générale, l'adresse IP ou l'URL du système concerné et une description de la vulnérabilité suffisent, mais des vulnérabilités plus complexes peuvent nécessiter davantage.
- Communiquer vos coordonnées afin que la CILE puisse vous recontacter et collaborer avec vous à une résolution sécurisée. Merci d'indiquer au minimum votre nom, votre adresse e-mail et/ou votre numéro de téléphone. Un signalement sous pseudonyme est possible, pour autant que la CILE dispose d'un moyen de vous contacter en cas de question complémentaire.
- Confirmer que vous avez agi et continuerez d'agir conformément à cette « Politique de divulgation ».

1.2.1 Règles que vous devez respecter

Les actions suivantes sont interdites :

- Divulguer la vulnérabilité avant qu'elle ne soit corrigée. Voir ci-dessous pour une éventuelle publication ultérieure.
- Abuser de la vulnérabilité en copiant, supprimant, modifiant ou visualisant inutilement des données ou, par exemple, en téléchargeant plus de données que nécessaire pour démontrer l'existence de la vulnérabilité.
- Installer des malware (virus, ver, cheval de Troie, etc.).
- Copier, modifier ou supprimer des données dans un système.
- Apporter des modifications au système.

- Accéder à plusieurs reprises au système ou partager l'accès avec d'autres.
- Utiliser des outils d'analyse automatisés.
- Utiliser des outils de « brute forcing ».
- Utiliser le déni de service ou l'ingénierie sociale (phishing, vishing, spam, …).
- Réaliser des actions qui pourraient avoir un éventuel impact sur le bon fonctionnement du système, tant en termes de disponibilité et de performances, mais également en termes de confidentialité et d'intégrité des données.
- Conserver les données obtenues via la vulnérabilité.

Les attaques concernant la sécurité physique ne sont pas tolérées.

Si vous souhaitez publier sur la vulnérabilité après sa suppression, il est demandé d'en informer la CILE au moins un mois avant la publication. L'identification, directement ou indirectement de la CILE dans une publication n'est possible qu'après accord préalable de celle-ci.

1.2.2 Engagement de la CILE

Si vous avez respecté les règles énoncées ci-dessus et qu'aucune autre infraction n'a été commise, la CILE s'engage à ne pas engager d'action en justice à votre encontre en lien avec le signalement effectué.

La CILE accusera réception de votre signalement dans les meilleurs délais et vous communiquera, dans la mesure du possible, une première évaluation ainsi qu'un calendrier prévisionnel de résolution.

Votre signalement sera traité de manière confidentielle. Aucune donnée personnelle ne sera transmise à des tiers sans votre autorisation, sauf si cette transmission est nécessaire pour respecter une obligation légale.

Vous serez tenu informé de l'évolution du traitement de la vulnérabilité signalée. La CILE mettra tout en œuvre pour résoudre le problème dans un délai raisonnable.

Pour toute question, vous pouvez nous contacter à l'adresse suivante : vulnerabilite@cile.be. Si des données confidentielles doivent être communiquées, celles-ci devront l'être via le lien sécurisé qui vous sera transmis.

Droit applicable : Le droit belge s'applique à tout litige relatif à l'application de la présente politique.

Entrée en vigueur et durée : La présente politique est applicable à partir du 1er juillet 2026 et demeure en vigueur jusqu'à sa modification ou son retrait par la CILE.