Politique de divulgation coordonnée des vulnérabilités

La ORES Assets S.C., dont le siège est sis à 6041 Gosselies, Avenue Jean Mermoz, 14, inscrite à la Banque-Carrefour des entreprises sous le numéro 0543.696.579 ; ici représentée par sa filiale ORES S.C., dont le siège est sis à 6041 Gosselies, Avenue Jean Mermoz, 14, inscrite à la Banque-Carrefour des entreprises sous le numéro 0897.436.971 ; société représentée par Stéphane Baldino, CISO (chief information security officer) et Vinciane Royez, DPO (data protection officer) ;

ci-après dénommée l' « organisation », a adopté la présente politique.

1. Le champ d'application de la politique

Soucieux d'améliorer la performance et la sécurité de nos réseaux et systèmes d'information, nous avons choisi d'adopter une politique de divulgation coordonnée des vulnérabilités. Celle-ci donne la possibilité aux participants de rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans les systèmes, les équipements et les produits de notre organisation ou de nous transmettre toute information découverte sur une vulnérabilité.

L'accès à nos systèmes et équipements informatiques est toutefois autorisé exclusivement avec l'intention d'en améliorer la sécurité, de nous informer des vulnérabilités existantes et dans le strict respect des autres conditions définies dans le présent document.

Notre politique concerne les vulnérabilités en matière de sécurité susceptibles d'être exploitées par des tiers ou de perturber le bon fonctionnement de nos produits, services, réseaux ou systèmes d'information.

Le divulgateur de vulnérabilités dispose également d'une autorisation d'introduire ou de tenter d'introduire des données informatiques dans notre système informatique, dans le respect des finalités et des conditions de la présente politique.

À savoir sur :

- les pages, formulaires web et services proposés sur le site www.ORES.be et autre services exposés par ORES sur internet ;

Par contre, sont strictement prohibés pour des raisons de sécurité et d'intégrité de ces réseaux, toutes tentatives sur le réseau de télécommunications d'ORES en ce compris, les installations électriques et gaz et équipements attenants (postes, cabines...) en gaz et électricité

Les systèmes qui dépendent de tiers sont exclus du champ d'application de la présente politique, sauf si ceux-ci marquent explicitement et préalablement leur accord sur les présentes règles. Par exemple, une solution SaaS n'entre pas dans le scope de cette politique de divulgation coordonnée des vulnérabilités car l'infrastructure est totalement gérée par un fournisseur. Si le divulgateur est en mesure de s'introduire dans la couche de virtualisation de service web, il doit préalablement demander l'accord d'ORES car, selon le type d'hébergement, cela pourrait avoir un impact sur d'autres entités/organismes.

Les recherches du participant sur des systèmes d'information non explicitement inclus dans le cadre de la présente politique pourraient entraîner des poursuites judiciaires à son encontre.

2. Les obligations réciproques des parties

a) La proportionnalité

Le divulgateur de vulnérabilités s'engage dans toutes ses actions à respecter scrupuleusement le principe de proportionnalité, c'est-à-dire à ne pas perturber la disponibilité des services fournis par le système et à ne pas faire usage de la vulnérabilité au-delà de ce qui est strictement nécessaire à la démonstration de la faille de sécurité. Son attitude doit rester proportionnée : si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin.

L'objectif de notre politique n'est pas de permettre la prise de connaissance intentionnelle du contenu de données informatiques, de données de communication ou de données à caractère personnel et une telle prise de connaissance ne pourrait intervenir que de manière fortuite dans le cadre de la recherche de vulnérabilités.

b) Les actions interdites

Le divulgateur de vulnérabilités ne peut recourir aux actions suivantes :

- la copie, la modification ou la suppression de données du système informatique ;
- la modification des paramètres du système informatique ;
- l'installation d'un logiciel malveillant (malware) : virus, vers (worm), chevaux de Troie (trojan horse, ou autre ;
- les attaques par déni de service (Distributed Denial Of Service - DDOS) ;
- les attaques par ingénierie sociale (social engineering) ;
- les attaques par hameçonnage (phishing) ;
- les attaques par courriels indésirables (spamming) ;
- le vol de mots de passe ou l'attaque en force de mots de passe (brute force) ;
- l'installation d'appareil permettant l'interception, la prise de connaissance ou l'enregistrement de communication non accessible au public ou d'une communication électronique ;
- l'interception, l'enregistrement ou la prise de connaissance intentionnelle d'une communication non accessible au public ou d'une communication électronique ;
- l'utilisation, la détention, la révélation, l'usage ou la divulgation intentionnelle du contenu de communications non accessibles au public ou de données d'un système informatique, dont le divulgateur de vulnérabilités ne peut raisonnablement ignorer qu'elles ont été obtenues illégalement ;

Si le divulgateur de vulnérabilités souhaite l'aide d'un tiers pour exécuter ses recherches, le divulagteur de vulnérabilités doit s'assurer que celui-ci prend préalablement connaissance de la présente politique et accepte, en offrant son assistance, d'en respecter les conditions.

De manière générale, le divulgateur de vulnérabilités s'interdira toute action susceptible d'interférer de manière directe ou indirecte avec le bon fonctionnement de nos systèmes et réseaux.

c) La confidentialité

Le divulgateur de vulnérabilités s'engage à ne pas partager ni divulguer à des tiers, de quelque manière que ce soit, les informations recueillies dans le cadre de notre politique, sauf accord préalable et explicite de notre part.

De même, il n'est pas permis de révéler ou de divulguer des données informatiques, des données de communication ou des données à caractère personnel à des tiers.

Dans le cas où la vulnérabilité peut également affecter d'autres organisations en Belgique, le divulgateur de vulnérabilités ou l'organisation responsable peuvent néanmoins en informer le CCB (vulnerabilityreport@cert.be).

d) L'exécution de bonne foi

Notre organisation s'engage à exécuter de bonne foi la présente politique et de ne pas poursuivre en justice, au civil ou au pénal, le divulgateur de vulnérabilités qui en respecte les conditions.

Le divulgateur de vulnérabilités doit être dénué d'intention frauduleuse, de dessein de nuire, de volonté de faire usage ou de provoquer un dommage au système visité ou encore à ses données. Cela vaut également pour les systèmes tiers situés en Belgique ou à l'étranger.

En cas de doute sur certaines des conditions de notre politique, le divulgateur de vulnérabilités doit interroger préalablement notre point de contact et obtenir son accord écrit avant d'agir.

e) Le traitement de données à caractère personnel

L'objet de cette n'est pas d'effectuer intentionnellement des traitements de données à caractère personnel mais il est possible que le divulgateur de vulnérabilités doive, même de manière fortuite, traiter des données à caractère personnel dans le cadre de ses recherches de vulnérabilités.

Or, le traitement de données à caractère personnel a une portée large et inclut notamment la conservation, la modification, l'extraction, la consultation, l'utilisation ou la communication de toute information pouvant se rapporter à une personne physique identifiée ou identifiable. Le caractère « identifiable » de la personne ne dépend pas de la simple volonté d'identification de celui qui traite les données mais de la possibilité d'identifier, directement ou indirectement, la personne à l'aide de ces données (par exemple : une adresse de courriel, numéro d'identification, identifiant en ligne, adresse IP ou encore des données de localisation).

Ainsi, il est possible que le divulgateur de vulnérabilités traite de manière limitée des données à caractère personnel. En cas de traitement de telles données, le divulgateur de vulnérabilités s'engage à respecter les obligations légales en matière de protection des données à caractère personnel[1] et les conditions de la présente politique, notamment :

- Le divulgateur de vulnérabilités s'engage à ne traiter des données à caractère personnel que selon les instructions de notre organisation, décrites dans la présente politique, et exclusivement afin de rechercher des vulnérabilités dans les systèmes, équipements ou produits de notre organisation. Tout traitement de données à caractère personnel pour une autre finalité est exclu.

- Le divulgateur de vulnérabilités s'engage à limiter le traitement de données à caractère personnel à ce qui est nécessaire au regard de la finalité de recherche de vulnérabilités.

- Le divulgateur de vulnérabilités veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

- Le divulgateur de vulnérabilités met en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (p.ex. cryptage). Le divulgateur de vulnérabilités déclare qu'il comprend les risques liés à la mise en œuvre de la présente politique et qu'il a l'expertise et l'expérience nécessaires afin de tester les systèmes, équipements et produits de notre organisation en toute sécurité et en respectant les lois et réglementations applicables.

- Le divulgateur de vulnérabilités s'engage à nous assister, dans la mesure du possible et compte tenu de la nature du traitement et des informations à la disposition du participant, dans la mise en œuvre de nos obligations relatives à l'exercice des droits des personnes concernées, la sécurité du traitement et toute analyse d'impact éventuelle.

- Le divulgateur de vulnérabilités s'engage à nous informer, dans les meilleurs délais après en avoir pris connaissance, de toute violation[2] éventuelle de données à caractère personnel à l'adresse vulnerabilites@ores.be.

- Le divulgateur de vulnérabilités ne peut conserver plus longtemps que nécessaire les éventuelles données à caractère personnel traitées. Durant cette période, le divulgateur de vulnérabilités doit veiller à ce que ces données soient conservées en garantissant un niveau de sécurité adapté aux risques encourus (de préférence de manière

1 Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD Règlement général sur la protection des données).

2 Une « violation de données à caractère personnel » consiste en une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données à caractère personnel.

encryptée). A l'issue de sa participation à la politique, ces données doivent être supprimés immédiatement.

- Le divulgateur de vulnérabilités s'engage à tenir un registre des catégories d'activités de traitement effectuées pour le compte de notre organisation comprenant notamment une description des mesures de sécurité qu'il a mises en œuvre, conformément à l'article 30, § 2 du RGPD.

3. Comment signaler les vulnérabilités de sécurité ?

a) Le point de contact

Vous devez adresser exclusivement les informations découvertes à l'adresse de courriel suivante : vulnérabilités@ores.be.

b) Les informations à transmettre

Dès que possible après la découverte, adressez-nous les informations sur vos découvertes en utilisant le formulaire repris en annexe I.

4. La procédure

a) Découverte

Lorsqu'un participant découvre des informations relatives à une vulnérabilité potentielle, celui-ci devrait, dans la mesure du possible, réaliser au préalable des vérifications permettant de confirmer l'existence de la vulnérabilité et d'identifier les éventuels risques encourus.

b) Notification

Le divulgateur de vulnérabilités s'engage à notifier, dans les plus brefs délais, les informations techniques sur les éventuelles vulnérabilités au point de contact [ou au coordinateur (optionnel)], repris au point 3 a) de la présente politique. Le divulgateur de vulnérabilités doit respecter les moyens de communication sécurisés désignés.

Lorsqu'elle reçoit une notification, notre organisation s'engage à envoyer au participant, dans les plus brefs délais, un accusé de réception, [avec si possible sa référence interne, un rappel des principales obligations de la Politique] et les étapes suivantes de la procédure.

c) Communication

Les parties s'engagent à mettre tout en œuvre pour assurer une communication continue et efficace. Les renseignements fournis par le divulgateur de vulnérabilités peuvent, en effet, s'avérer très utiles pour identifier la vulnérabilité, y apporter une solution.

En l'absence de réaction de l'une des parties à la CVDP au-delà d'un délai raisonnable, les parties peuvent faire appel au Centre pour la Cybersécurité Belgique (CBB) (vulnerabilityreport@cert.be), comme coordinateur (par défaut).

d) Investigation

La phase d'investigation permettra à notre organisation de reproduire l'environnement et le comportement signalé afin de vérifier les informations communiquées.

Notre organisation s'engage à tenir informé de manière régulière le divulgateur de vulnérabilités des résultats des investigations et des suites données à sa notification.

Durant ce processus, les parties veilleront à faire le lien avec les notifications similaires ou connexes, d'évaluer le risque et la gravité de la vulnérabilité, et de détermination les éventuels autres produits ou systèmes affectés.

e) Développement d'une solution

L'objectif de la politique de divulgation est de permettre le développement d'une solution afin de faire disparaître la vulnérabilité du système informatique, avant que des dommages ne soient causés.

En tenant compte de l'état des connaissances, des coûts de mise en œuvre, de la gravité des risques encourus par les utilisateurs et des contraintes techniques, notre organisation tentera de mettre au point une solution au plus tard dans les 90 jours calendrier.

Dans cette phase, notre organisation et ses partenaires s'engagent à mener, d'une part, des tests positifs pour vérifier que la solution fonctionne correctement et, d'autre part, des tests négatifs pour s'assurer que la solution ne perturbe pas le bon fonctionnement des autres fonctionnalités existantes.

f) Éventuelle divulgation publique

Notre organisation décidera, en coordination avec le divulgateur de vulnérabilités, des modalités pour rendre éventuellement public l'existence de la vulnérabilité. Cette divulgation publique devra se faire au plus tôt en même temps que le déploiement d'une solution et la diffusion d'un avis de sécurité destiné aux utilisateurs.

Dans l'hypothèse d'une vulnérabilité qui concernerait également d'autres organisations, l'organisation responsable se doit d'en informer, en tout état de cause, le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be), même si elle ne souhaite pas que la vulnérabilité soit divulguée publiquement.

Notre organisation s'engage également à recueillir les commentaires des utilisateurs sur le déploiement de la solution et de prendre les mesures correctives nécessaires pour régler les éventuels problèmes posés par la solution, notamment de compatibilité avec d'autres produits ou services.

5. Droit applicable

Le droit belge est applicable aux litiges liées à l'application de la présente politique.

Le CCB (vulnerabilityreport@cert.be) peut servir d'intermédiaire pour tenter de concilier notre organisation et le divulgateur de vulnérabilités pour les problèmes liés à l'application de la présente politique].

6. Durée

Les règles de la politique sont applicables à partir du 04/08/2025 jusqu'à leur éventuelle modification ou suppression par notre organisation. Ces modifications ou suppressions seront publiées sur le site internet de notre organisation et s'appliqueront automatiquement après un délai de 30 jours après leur publication.

Annexe I : Formulaire de notification de vulnérabilités

Fournissez suffisamment d'informations pour nous permettre de reproduire le problème et de le résoudre le plus rapidement possible.

Nous vous demandons de nous fournir au moins les informations pertinentes suivantes :

Nom : **Prénom :**	
(Adresse/Pays) :	
Adresse de courriel : **Numéro de téléphone :**	
Description de la vulnérabilité :	
Type de vulnérabilité :	
Détails de la configuration :	
Système d'exploitation :	

Opérations effectuées (logs) :	
Outils utilisés :	
Dates et heures des tests :	
Adresse IP ou de l'URL du système affecté :	
En cas de traitement de données personnelles :	• Types de données personnelles consultées/traitées : • Catégories de personnes concernées (client, employé, fournisseur) : • Transfert de données vers/accès depuis un pays situé en dehors de l'Union européenne ou de l'Espace économique européen ? Si oui: - indiquez le(s) pays concerné(s) : - retournez l'Annexe II complétée et signée.
Toute autre information pertinente :	
Annexes (captures d'écran) :	

Que faisons-nous avec vos données à caractère personnel ?

Nous vous invitons à lire notre politique de protection des données à caractère personnel disponible ici : https://www.ores.be/notice-vie-privee.