Divulgation de vulnérabilités

Version 1.3 | Dernière mise à jour : 29 septembre 2026

La sécurité de nos systèmes s'améliore aussi grâce aux personnes qui prennent le temps de nous signaler une faille. Cette politique dit ce que nous attendons d'un signalement, ce que nous nous engageons à en faire, et dans quel cadre légal belge il s'inscrit.

Périmètre

Sont couverts les systèmes exploités par Avanserv SRL pour son propre compte : le site avanserv.com, l'application app.avanserv.com et son API, ainsi que l'infrastructure qui les sert. Ne sont pas couverts les systèmes et applications de nos clients, même lorsque nous les hébergeons : ils appartiennent à leurs propriétaires et toute recherche y requiert l'autorisation de ceux-ci.

Les règles du jeu

Limitez vos investigations à ce qui est nécessaire pour démontrer la vulnérabilité et arrêtez-vous à la première preuve. N'exfiltrez pas de données au-delà de cette preuve, ne modifiez et ne supprimez rien, ne dégradez pas le service : les attaques par déni de service, l'ingénierie sociale, le phishing et les intrusions physiques sont hors du cadre de cette politique. Ne divulguez rien publiquement avant la fin de la coordination décrite ci-dessous.

Comment signaler

Écrivez à security@avanserv.com en décrivant la vulnérabilité, les étapes permettant de la reproduire, l'impact que vous en estimez et, si vous le souhaitez, un moyen de vous créditer. Pour bénéficier de la protection légale décrite plus bas, signalez-la aussi, selon la procédure publiée par le Centre pour la Cybersécurité Belgique (CCB) : un signalement simplifié dans les 24 heures de la découverte, puis un signalement complet dans les 72 heures. Nous écrire seuls ne suffit pas à obtenir cette protection.

Nous accusons réception dans les cinq jours ouvrables, nous vous tenons informé de l'avancement, et nous visons une correction dans un délai proportionné à la gravité. Nous convenons ensemble d'une date de publication, avec un horizon par défaut de 90 jours calendrier après le signalement, étant entendu que cette date reste soumise à l'accord du Centre pour la Cybersécurité Belgique. Avec votre accord, nous créditons volontiers votre contribution ; nous n'opérons pas de programme de récompenses.

Le cadre légal belge

Le droit belge protège la recherche de vulnérabilités menée de bonne foi. En vertu des articles 22 et 23 de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information, une personne qui découvre une vulnérabilité peut bénéficier d'une protection légale si elle agit sans intention frauduleuse ni volonté de nuire, si elle ne va pas au-delà de ce qui est nécessaire et proportionné pour établir l'existence de la vulnérabilité, si elle adresse un signalement simplifié dans les 24 heures de sa découverte puis un signalement complet dans les 72 heures, au Centre pour la Cybersécurité Belgique (CCB) ainsi qu'à l'organisation concernée, et si elle ne divulgue rien publiquement sans l'accord du CCB. Les modalités de signalement au CCB sont publiées sur ccb.belgium.be. La présente politique vaut, pour nos propres systèmes, adhésion à ce cadre : nous ne déposerons pas plainte et n'engagerons aucune action civile contre une recherche respectant ces conditions et les règles ci-dessus.

Le fichier security.txt

Un fichier conforme à la RFC 9116 est publié à l'adresse https://avanserv.com/.well-known/security.txt. Il indique l'adresse indiquée ci-dessus, cette page comme politique applicable, le français et l'anglais comme langues de lecture, ainsi qu'une date d'expiration que le site renouvelle à chaque construction du site. La politique qu'il désigne couvre les deux systèmes, le site et l'application, comme l'indique la section sur le périmètre.

Il n'est pas reproduit ici. Une adresse de contact écrite deux fois est une adresse qu'une modification peut laisser dans deux états, et c'est le fichier que lisent les machines.