InterSystems officiel
Robert Bira · Jan 31, 2023

Mise à jour de la politique de gestion des vulnérabilités

Chez InterSystems, nous croyons en la divulgation responsable des vulnérabilités de sécurité récemment découvertes. Nous fournissons des informations opportunes à nos clients, tout en les gardant hors de la portée des personnes susceptibles d'en faire un mauvais usage. Nous comprenons également que chaque client a des exigences différentes liées à la résolution des problèmes de sécurité.

Alors que nous commençons 2023, nous avons apporté deux changements importants à notre approche des corrections des failles de sécurité que je voudrais souligner :

1. Des correctifs de vulnérabilité de sécurité seront inclus dans chaque version
2. Notification client améliorée

Correctifs de vulnérabilité de sécurité dans chaque version

Au lieu d'attendre de fournir des correctifs dans une version de sécurité, chaque version peut désormais inclure des correctifs pour les vulnérabilités de sécurité. Notre cadence de publication améliorée fournira des correctifs sur le terrain en temps opportun.

Notification client améliorée

Les éléments à impact faible et moyen, qui incluent souvent des vulnérabilités telles que les attaques de reconnaissance ou les attaques de script intersite, seront inclus dans chaque version et décrits dans les notes de version du produit.

Les correctifs pour les éléments de gravité supérieure seront également inclus dans chaque version dès qu'ils seront prêts, mais les informations concernant le correctif seront sous embargo jusqu'à ce que les correctifs soient dans toutes les versions prises en charge.

Une alerte de sécurité sera publiée pour les problèmes de gravité élevée et critique lorsqu'ils auront été corrigés dans toutes les versions prises en charge.

Pourquoi InterSystems a-t-il apporté ces changements ?

Nous pensons que ces améliorations vont :

1. Transmettre plus rapidement les correctifs de sécurité à nos clients
2. Aider à se concentrer sur les correctifs les plus graves
3. Rendre possible, dans certains cas, de fournir des correctifs de sécurité sous forme de correctifs au lieu de kits complets
4. Fournir plus de transparence sur la façon dont les vulnérabilités de sécurité sont gérées en regroupant les vulnérabilités en fonction de leur impact sur la sécurité
5. Autoriser les administrateurs système à appliquer davantage de correctifs en fonction de leurs besoins et de leurs exigences

Bien sûr, le processus devient beaucoup plus compliqué avec la notion de versions de maintenance et de livraison continue. Afin d'aider les clients à comprendre quand et comment ils peuvent obtenir des correctifs de sécurité, nous avons publié notre politique de gestion des vulnérabilités avec des informations plus détaillées.

J'attends avec impatience 2023 où nous pourrons continuer à améliorer votre expérience liée à notre programme de gestion de la sécurité et des vulnérabilités.

#Sécurité #InterSystems IRIS #InterSystems IRIS for Health #InterSystems officiel