Informations vulnérabilité Log4j

Sage et ses partenaires prennent la sécurité de ses solutions et de ses clients très au sérieux.

A ce titre et dans le cadre de sa politique de sécurité, Sage entreprend régulièrement des tests proactifs sur ses produits pour identifier les vulnérabilités potentielles et fournir des correctifs.

Suite à l'annonce initiale de la vulnérabilité Apache Log4j le 10 décembre et aux mises à jour ultérieures, Sage a étudié l'impact potentiel sur nos produits et services :

Gamme	Produit	Vulnérabilité potentielle
Bâtiment	Multi Devis Entreprise Batigest I7 et Connect Sage E Chantier Alobees Bi Reporting Sage e-tarif - Tariféo	Non
Ciel et Sage 50	Toutes les solutions hors Ciel Paye	
Sage 100	Toutes les solutions Sage 100 hors CRM et Sage recouvrement créances	
Etats Comptables et Fiscaux	Etats Comptables et Fiscaux	
Fa7	Toutes les solutions	
Sage Business Cloud	Sage Business Cloud Comptabilité	
	Bureau	
Sage Petites Entreprises	Toutes les solutions	
Sage XRT Business Exchange	SBE	
Sage XRT Treasury	Toutes les solutions	
Sage XRT Advanced	Toutes les solutions	
Sage FRP 1000	Toutes les solutions Sage FRP1000 (y compris Sage FRP 1000 Dématérialisation Saas)	
Sage Experts	Toutes les solutions	

Gamme	Produit	Vulnérabilité potentielle	Correctif livré	Informations Log4j
Solutions de Paie	Ciel Paye Sage 100 Paye & RH Sage Business Cloud Paie Sage Service Paie Déclarations Sociales	Indirecte	Oui	La solution de Paye utilise un outil de contrôle de fichiers DSN mis à disposition par la CNAV. Cet outil a été impacté par une faille potentielle Log4j, néanmoins mineure et maîtrisée. La CNAV a mis à disposition un correctif, et les équipes Sage se sont chargées de mettre à jour automatiquement les serveurs utilisant cet outil de contrôle (le 31/01/22). Vous n'avez donc aucune intervention à réaliser de votre côté.
Sage 100	CRM	Oui	Oui	Une faille potentielle est présente sur la version 8.00. Veuillez mettre à jour votre solution dans la dernière version 8.05 disponible depuis le 22 décembre (My Sage ou Partner Hub)
	Sage Recouvrement Créances	Indirecte	Oui	La solution Sage Recouvrement Créances n'est pas directement impactée par une vulnérabilité Log4j. Le connecteur est protégé de toute tentative de connexion entrante, même s'il utilise des bibliothèques Java potentiellement impactées. C'est la raison pour laquelle ce connecteur a été ajusté depuis le 14/01/22 afin de maximiser la protection. Nous vous invitons à l'installer depuis le menu "Aide et Support" > "Installation",
Sage Espace Employés	Sage Espace Employés	Oui	Oui	Une version corrective a été automatiquement déployée. Aucune intervention de votre part n'est nécessaire.
Sage FRP 1000	Sage FRP 1000 Dématérialisation on-premise	Oui	Oui	Une faille potentielle est présente sur la version FRP 1000 Dématérialisation (la version Saas n'est pas concernée). Afin d'assurer la sécurité de la solution, il est nécessaire de mettre à jour la version On-Premise de Sage 1000 Dématérialisation. Pour cela, au lancement de votre application, vous serez informé qu'une mise à jour est disponible. Une action manuelle est requise en cliquant sur le bouton "Télécharger" présent sur l'interface client. Il suffira de suivre les indications mentionnées pour clôturer cette mise à jour essentielle.
Sage X3	Toutes les solutions	Note d'information		Le logiciel Sage X3 n'est pas exposé à la vulnérabilité Apache Log4j, cependant, Sage X3 s'intègre nativement à une solution tiers appelée Elasticsearch. Les versions 11 et 12 de Sage X3 sont susceptibles d'être intégrées à des instances d'Elasticsearch concernées (par exemple, la version 7.9 et supérieure), mais ne sont pas exposées si les bonnes pratiques de sécurité recommandées par Sage et pour Sage X3 ont été respectées. Par conséquent, nous vous encourageons à vérifier votre installation Elasticsearch et à appliquer la correction de sécurité mise à disposition par Elastic.Vous trouverez par ailleurs les informations et conseils sur les bonnes pratiques de sécurité de Sage X3 dans l'aide en ligne de Sage X3.

Date de mise à jour du document 08/02/2022