Sécurité de sedex : vulnérabilité mondiale CVE-2026-91403

2026-10-29 - Florian Cattin - Commentaires (0) - Communes

Madame, Monsieur,

Prime Technologies a appliqué les recommandations les plus exigeantes relatives à la mise à jour de sedex. Lundi 26.10.2026, 11h, la version 8.0.6 était installée pour la totalité de nos clients l'utilisant.

Ci-dessous figure la communication du 29.10.2026 de l'OFS, concernant la vulnérabilité mondiale CVE-2026-91403, qui expose les résultats de son analyse approfondie :

> *Dans notre première communication, nous étions partis, par précaution, d'une possible exposition, l'analyse approfondie n'étant pas encore terminée à ce moment-là. Cette analyse est désormais terminée et ses résultats sont présentés ci-dessous.*
>
> *Conclusion essentielle : la sécurité des échanges sedex n'a à aucun moment été compromise par cette vulnérabilité. Notre analyse détaillée a confirmé que des mécanismes de protection supplémentaires, déjà présents dans les versions antérieures du client sedex, empêchent l'exploitation de cette vulnérabilité dans les communications sedex.*
>
> ***Pourquoi sedex est-il protégé ?***
>
> *Pour vérifier les certificats des serveurs lors des connexions TLS, le client sedex n'utilise pas le truststore général du système d'exploitation ou de Java. Il utilise son propre truststore dédié et soigneusement sélectionné, qui ne contient que des certificats et autorités de certification de l'OFIT et de la Swiss Government PKI. Ce truststore peut en outre être mis à jour automatiquement. Les autorités de certification compromises dans le cadre de CVE-2026-91403 n'en font pas partie. Le sedex Web Service Proxy utilise également un truststore de confiance dédié.*
>
> *De plus, sedex utilise des certificats X.509 distincts pour deux fonctions de sécurité : les certificats de point de terminaison TLS protègent la connexion entre le client et le serveur sedex, tandis que les certificats des participants sedex assurent le chiffrement de bout en bout des messages entre participants. Ces derniers n'appartiennent pas à l'infrastructure de certificats Internet concernée par cet incident. Le chiffrement de bout en bout n'a donc jamais été affecté.*
>
> ***Pourquoi avons-nous néanmoins publié une mise à jour ?***
>
> *La sécurité est notre priorité absolue. Dès que cette vulnérabilité mondiale a été connue, nous avons réagi rapidement et publié le client sedex 8.0.6 pour Windows et Docker, par mesure de précaution. Cette version actualise principalement les restrictions de confiance de l'environnement d'exécution Java afin d'exclure explicitement les autorités de certification compromises. Quelques bibliothèques utilisées par sedex ont également été actualisées indépendamment de cet incident.*
>
> *Ces précautions sont utiles à la sécurité globale des installations, même si notre analyse approfondie montre qu'une attaque fondée sur CVE-2026-91403 ne peut pas être exploitée contre les communications sedex.* [Source : OFS, sedex Newsmail]

Pièce jointes

- OFS-sedex-Information-CVE-2026-91403.pdf [152.44 KB]