



## Analyse de sécurité / Sicherheitsanalyse / Analisi di sicurezza CVE-2026-91403

### Français

Madame, Monsieur,

À la suite de notre communication concernant la vulnérabilité mondiale **CVE-2026-91403** dans l'infrastructure de confiance des certificats, le support sedex a reçu de nombreuses questions sur la sécurité de sedex. Nous souhaitons y répondre et vous informer des résultats de notre 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. Les changements sont détaillés dans les [Release Notes](#).

## Questions fréquentes

### 1. sedex est-il concerné par CVE-2026-91403 ?

Non. Le client sedex et le sedex Web Service Proxy utilisent des truststores de confiance dédiés, contenant exclusivement des autorités de certification de l'OFIT et de la Swiss Government PKI. Les autorités de certification compromises dans le cadre de CVE-2026-91403 n'y figurent pas. Il est donc impossible d'exploiter cette vulnérabilité pour usurper l'identité d'un serveur sedex.

### 2. Quelles sont les conséquences pour le client sedex ?

Notre analyse approfondie n'a révélé aucune possibilité d'exploiter cette vulnérabilité dans les échanges sedex. La confidentialité du chiffrement de bout en bout des messages est en outre assurée indépendamment de la connexion TLS.

### 3. La nouvelle version corrige-t-elle également la vulnérabilité PHP signalée à peu près au même moment ?

Cette vulnérabilité est indépendante de CVE-2026-91403. sedex n'utilise aucun composant PHP, ni dans le client ni côté serveur. sedex n'est donc pas concerné par cette vulnérabilité PHP.

### 4. Dois-je actualiser le client si j'ai déjà appliqué la solution transitoire avec blocked.certs ?

Une mise à jour immédiate n'est pas nécessaire en raison de cet incident. Nous recommandons néanmoins d'installer la version actuelle lors d'une prochaine fenêtre de maintenance, afin de maintenir l'ensemble des composants à jour. Voir les [Release Notes](#).

### 5. Les anciennes versions, notamment sedex 7.0.0, étaient-elles concernées ?

Non. Toutes les versions du client sedex actuellement en service disposent du mécanisme de protection supplémentaire reposant sur un truststore de confiance dédié.

### 6. La mise à jour est-elle impérative ou urgente ?

Il n'y a, sur la base de l'analyse actuelle, **aucune urgence particulière liée à CVE-2026-91403**. Nous recommandons une mise à jour planifiée dans le cadre de la maintenance habituelle.

### 7. Quels risques subsistent si je ne procède pas immédiatement à la mise à jour ?

La vulnérabilité décrite ne représente pas de menace directe pour les communications sedex grâce aux mécanismes de sécurité supplémentaires. Il reste toutefois important de corriger régulièrement les vulnérabilités connues de tous les composants logiciels, afin de réduire les risques d'autres scénarios d'attaque, notamment de combinaisons de faiblesses.

## Recommandation et support

Nous recommandons d'installer **le client sedex 8.0.6 pour Windows ou Docker** dans le cadre d'une prochaine maintenance, sans intervention d'urgence. Sous **Linux**, l'environnement d'exécution Java est fourni par l'exploitant : il doit donc être maintenu à jour séparément, indépendamment de la version du client sedex. Pour d'autres applications Java de votre infrastructure, CVE-2026-91403 peut en revanche rester pertinente : nous recommandons de les mettre à jour conformément aux indications de leurs fournisseurs. Les autres composants de l'infrastructure doivent eux aussi suivre les processus habituels de gestion des correctifs de sécurité.

Pour toute question, le support sedex se tient à votre disposition : [sedexsupport@bfs.admin.ch](mailto:sedexsupport@bfs.admin.ch).

Nous vous remercions de votre contribution à la sécurité durable de sedex.

Meilleures salutations  
sedex Support