

Avis de Sécurité sur le Terrain (FSN) Sectra Core

Cet avis de sécurité contient des informations importantes concernant Sectra Core.

Sectra demande à tous les clients recevant cet avis de suivre les actions décrites ci-dessous.

Champ d'application	Clients ayant reçu cet avis de sécurité (FSN).
Destinataires	Personne(s) responsable(s) du système Sectra PACS (Sectra Core) au sein des établissements de santé.
Référence FSN	DOC-LHEN-DMBC9R
Référence FSCA	DOC-LHEN-DMBC7S
Incident identifié	Sectra a identifié une vulnérabilité critique lors du développement du logiciel. À ce jour, Sectra n'a connaissance d'aucune exploitation de cette vulnérabilité.
Produit et versions concernés	Sectra PACS (Sectra Core), toutes les versions antérieures à la version 27.2.
Description du problème	Une vulnérabilité critique a été découverte dans Sectra Core. Une exploitation réussie pourrait permettre l'exécution de code à distance (RCE) sur le serveur exécutant le service.
Conséquences cliniques	Cette vulnérabilité pourrait entraîner une perte de confidentialité, d'intégrité et de disponibilité des informations de santé des patients. Les implications cliniques incluent, entre autres, des retards ou des erreurs dans le traitement ou le diagnostic
Actions à entreprendre par le client	Appliquer le correctif (patch) dès que possible.
Actions prises par Sectra	Sectra a publié des correctifs (mises à jour logicielles) pour toutes les versions prises en charge.
Compte rendu	Toutes les organisations recevant cet avis doivent contacter leur représentant Sectra désigné dès que possible afin de planifier une fenêtre de maintenance pour l'application du correctif.
Informations complémentaires	

Veuillez contacter votre représentant Sectra si vous avez des questions concernant cet avis.

Linköping 2025-10-17

Johan Sjöberg
Product Manager, Sectra Core Server Platform

Helene Fogelberg
Chief Quality Officer