Field Safety Notice (FSN) Sectra Core

This FSN contains important safety information regarding Sectra Core.
Sectra urges all customers that receive this FSN to take the actions described below.

Scope	Customers that receive this FSN.
Attention	Person(s) responsible for Sectra PACS (Sectra Core) at healthcare organizations.
FSN reference	DOC-LHEN-DMBC9R
FSCA reference	DOC-LHEN-DMBC7S
This has happened	Sectra has identified a critical vulnerability during software development. Currently, Sectra is not aware of any exploitation of the vulnerability.
Affected product and versions	Sectra PACS (Sectra Core), all versions prior 27.2.
Description of product problem	A critical vulnerability has been found in Sectra Core. Successful exploitation may lead to remote code execution (RCE) on the server running the service.
Clinical implications	Loss of Confidentiality, Integrity and Availability of patient health information. Clinical implications include, but are not limited to, delayed or incorrect treatment or diagnosis.
You must take the following actions	Apply patch as soon as possible.
Sectra to take the following actions	Sectra has published patches (software updates) for all supported versions.
Reporting back	All organizations receiving this notice must contact the designated Sectra customer representative as soon as possible to plan a service window for applying patch.
Additional information	

Please contact your Sectra customer representative if you have any questions regarding this notice.

Linköping 2025-10-14

Johan Sjöberg
Product Manager, Sectra Core Server Platform

Helene Fogelberg
Chief Quality Officer