Nexans switch firmware, manager and Spring4Shell vulnerability

KD1831E0

Vulnerability background

CVE-2022-22965 (Spring4Shell, SpringShell) is a vulnerability in the Spring Framework that uses data binding functionality to bind data stored within an HTTP request to certain objects used by an application. The bug exists in the getCachedIntrospectionResults method, which can be used to gain unauthorized access to such objects by passing their class names via an HTTP request. It creates the risks of data leakage and remote code execution when special object classes are used. This vulnerability is similar to the long-closed CVE-2010-1622, where class name checks were added as a fix so that the name did not match classLoader or protectionDomain.

Nexans switches unaffected

Nexans is NOT exposed to the Spring4Shell vulnerability.

All types of Nexans switch firmware and manager software versions are unaffected because Nexans doesn't use the Spring Framework.

Advanced Networking Solutions GmbH

Issued in 07.04.2022, Mönchengladbach Germany