

## Components:

aveva work tasks 2020  
aveva manufacturing execution system 2020  
aveva platform common services 4.4.6  
aveva enterprise data management 2021  
aveva platform common services 4.5.2  
aveva batch management 2020  
aveva mobile operator 2020  
aveva platform common services 4.5.0  
aveva platform common services 4.5.1  
aveva system platform 2020

## Description:

The vulnerability, if exploited, could allow a malicious entity with access to the file system to achieve arbitrary code execution and privilege escalation by tricking AVEVA Edge to load an unsafe DLL.

## Main problems:

427 "Uncontrolled Search Path Element"