

kardex kardex control center 5.7.12\+0-a203c2a213-master

Description:

Kardex Mlog MCC 5.7.12+0-a203c2a213-master allows remote code execution. It spawns a web interface listening on port 8088. A user-controllable path is handed to a path-concatenation method (Path.Combine from .NET) without proper sanitisation. This yields the possibility of including local files, as well as remote files on SMB shares. If one provides a file with the extension .t4, it is rendered with the .NET templating engine mono/t4, which can execute code.

Main problems:

94 "Improper Control of Generation of Code ('Code Injection')"