Software Assurance Tips

A product of the Software Assurance Tips Team[**swatips**]

Kevin Keen

Monday 18th April, 2022

1 Improper Resource Access Authorization

Updated Monday 18th April, 2022

Part of being a cyber security specialist is knowing the tools we use and what they are trying to communicate. Sometimes that is not as clear as we would wish. Take for example the finding of *Improper Resource Access Authorization* produced by Checkmarx. This is perhaps one of my least favorite findings as it tends to be very noisy, flagging on nearly any I/O that the application performs. What is it that the scanner is trying to tell us here? Let's look at the corresponding CWE according to Checkmarx. The documentation from Checkmarx maps this finding to *CWE-285: Improper Authorization*. The short description reads: "The software does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action."

That may be a bit too general, but the gist of it is that the scanner is attempting to ask "Does the user of the application have authorization to access the resource that is the target of this I/O operation?" In nearly every case we do not have enough information from the code alone to answer that question. In a few cases, the application may have the concept of users, and there might be a user check guarding the I/O. Only in those cases do we have a chance at marking these findings a `false positive`. But more often, the application has no notion of separate user roles. At that point there is no way to answer this question from the code alone. It becomes something that must be answered by policy or external documentation.

Note that a similar sounding finding from Checkmarx, Exposure of Resource to Wrong Sphere, is a completely different issue dealing with whether public variables are marked final.