

How to know if configuration files should be trusted



This page has been made public for vendors

Question

Fortify has flagged data read from a configuration file as potentially tainted. I trust files on my filesystem. How can I know that it is trusted?

Answer

Fortify views all data that comes from outside an application as a potential vector for an attack. It therefore marks all data coming into an application as potentially tainted and requires the data to be validated before it is used.

Best practice is to not trust files on the filesystem. Vulnerabilities in the operating system, other applications running on the server, and misconfiguration can all lead to compromise of those files. All data should be validated close to where it is used, including data that is read from configuration files. This best practice helps ensure all data is validated and that it is validated correctly for how it will be used. Alternatively, integrity checks can be implemented to verify that a configuration file has not been modified by an unauthorized party.

While best practices should be followed whenever possible, the Software Assurance Team recognizes that this is not always feasible in all cases for all applications. For example, in some applications it is not possible to validate paths read from the configuration file. When it is not possible to follow the best practices described above, the developer can show that the file is adequately protected as follows:

- The developer will need to provide documentation that attests that the server hosting the application is configured and operated securely according to VA hosting facility policy and that the files in question are protected from unauthorized read and/or write access
- The file is not generated or modified by another software application

References

- [VA Secure Code Review SOP](#)

Request code review tools, validations, and support [HERE](#).