

How to troubleshoot "Function...is too complex" errors



This page has been made public for vendors

Question

How do I resolve issues reported by the Fortify scan of the form: "Function...is too complex"?

Some of these issues include:

- "Function . . . is too complex for exhaustive dataflow analysis and further analysis will be skipped (visits)"
- "Function . . . is too complex for exhaustive dataflow analysis and further analysis will be skipped (time)"
- "Function . . . is too complex for exhaustive dataflow analysis and further analysis will be skipped (stack)"
- "Function . . . is too complex for controlflow analysis and will be skipped. (time) "

Answer

The depth of analysis Fortify SCA performs sometimes depends on the resources available and allocated to Fortify SCA on the computer where the scan is being performed. If Fortify SCA detects that it does not have enough resources available when scanning a particular function, then one or more of these issue may be reported.

The resources allocated to Fortify SCA's control flow and dataflow analysis engines can be limited by specifying values for Fortify SCA properties and/or options known as limiters. Fortify has four types of resource limiters that may affect these analysis engines:

1. Number of distinct locations (visits)
2. Memory
3. Stack size
4. Time

To resolve these errors, the developer should increase the property or option values associated with these resource limiters to a point where the analysis can complete successfully. If it is necessary to increase a limit beyond a reasonable amount (e.g., beyond available memory or it adds many hours to the scan), then the developer should include a readme file with the V&V secure code review package that explains what steps were taken to resolve the issue and why it was not possible to resolve it. This will be taken into consideration during the review.

A full description of how resource limits may be adjusted is provided in the [HPE Security Fortify Static Code Analyzer Performance Guide](#). A summary of that information is provided here.

For **Memory** and **Stack size** resource limits, the memory and stack space allocated to Fortify must be increased using the `-Xmx` and `-Xss` command-line options, respectively. More information on increasing memory is available in the technical note [How to increase memory for Fortify to do translation](#).

The remaining resource limits are adjusted using properties. These properties may be set in the `fortify-sca.properties` file (see the [User Guide](#) for the location of this file) or it may be set on the command line using the `-D` option.

The Dataflow **Number of distinct locations** limit is set using a combination of the three properties shown below. Please see the Fortify SCA Performance and User Guides for more information on how these properties interact. The values shown are the default limits:

```
com.fortify.sca.limiters.MaxTaintDefForVar = 1000

com.fortify.sca.limiters.MaxTaintDefForVarAbort =
4000
com.fortify.sca.limiters.MaxFieldDepth = 4
```

| | |
|-------------------------|--|
| HPE Fortify Version | 16.11 and later |
| Programming Language | <input checked="" type="checkbox"/> C/C++ <input checked="" type="checkbox"/> .NET <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> Objective -C <input checked="" type="checkbox"/> Other |
| Fortify Audit Workbench | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Fortify IDE Plugin | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Other Fortify Component | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

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

The Control flow **Time** limit may be set directly with a single property as shown with its default limit (in milliseconds) below. At this default setting, the Control flow analysis engine will abort analysis of a function that takes longer than 10 minutes (600000 milliseconds):

```
com.fortify.sca.CtrlflowMaxFunctionTime = 600000
```

If scanning from one of the graphical interfaces, please see the technical note on [how to enter command-line arguments into Audit Workbench or Fortify IDE plugin](#).

References

- HPE Security Fortify Static Code Analyzer Performance Guide, Chapter 6
Function too Complex to Analyze Message
- HPE Security Fortify Static Code Analyzer User Guide, Appendix I,
Configuration Options