

This repository | Search

Pull requests | Issues | Gist

Microsoft / binskim

Watch

60

★ Unstar

163

Fork

37

<> Code

🔔 Issues 13

🔗 Pull requests 1

📁 Projects 0

📖 Wiki

📈 Pulse

📊 Graphs

A binary static analysis tool that provides security and correctness results for Windows portable executables.

📌 147 commits

🌿 14 branches

📦 0 releases

👤 7 contributors

📄 MIT

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

👤 michaelcfanning committed on GitHub Merge pull request #71 from Microsoft/1-3-9

Latest commit 5235741 28 days ago

📖 README.md

BinSkim Binary Analyzer

This repository contains source code for BinSkim, a portable executable scanner that validates compiler/linker settings and other security-relevant binary characteristics.

Getting Started as a Developer

1. Clone the repository
2. Load and compile src\BinSkim.sln

Execute output in bld\bin\BinSkim.Driver for testing.

Submitting Pull Requests

Run test.cmd at the root of the enlistment to ensure that all tests pass, and x64 and x86 release builds succeed.

Getting Started as a User

Download BinSkim from Nuget

Latest stable Nuget version: [1.3.8](#)

Command-Line Documentation

-o, --output File path to which analysis output will be written.

-v, --verbose Emit verbose output. The resulting comprehensive report is designed to provide appropriate evidence for compliance scenarios.

-r, --recurse Recurse into subdirectories when evaluating file specifier arguments.

-p, --policy Path to policy file that will be used to configure analysis. Pass value of 'default' to use built-in settings.

-s, --statistics Generate timing and other statistics for analysis session.

-h, --hashes Output SHA-256 hash of analysis targets when emitting SARIF reports.

--sympath Symbols path value, e.g., SRV<http://msdl.microsoft.com/download/symbols> or
Cached:\symbols;Srv**http://symweb

--help Display this help screen.

--version Display version information.

value pos. 0 One or more specifiers to a file, directory, or filter pattern that resolves to one or more binaries to analyze.

Example Command-Line

```
binsskim.exe c:\bld*.dll --recurse --policy default --output MyRun.sarif
```

See the [SARIF](#) site for more information on the 'Static Analysis Results Interchange Format'

