Code::Blocks Tickets

A free C, C++ and Fortran IDE

Brought to you by: killerbot, mandrav, mortenmacfly, thomas-denk

#934 Buffer overflow in the way project files are processed

Milestone: Undefined **Status:** invalid **Owner:** nobody **Labels:** None
Type: Bug_Report
Updated: 2022-08-18 **Created:** 2020-03-28 **Creator:** Vilius Povilaika **Private:** No

To replicate the buffer overflow:
1. Create a new CBP project
2. Close the project, open the .cbp file with a text editor
3. Find the object_output setting in the Debug configuration
4. Replace the value with 6 thousand characters
5. Load the file into Code::Blocks IDE
6. Press 'Build and Run'
7. Watch your program crash

Discussion

Vilius Povilaika - *2020-04-09*

Detailed instructions on replication can be found here:
https://www.povonsec.com/codeblocks-security-vulnerability/

Miguel Gimenez - *2021-12-02*

- **status**: open --> invalid

John Helmert III - *2022-08-18*

Hi, why was this closed as invalid? I can definitely reproduce (despite the relatively poor report).

ollydbg - *2022-08-18*

The report has some issue:
1, "6 thousand characters"???
2, we web address is broken, I can't access it.

John Helmert III - *2022-08-18*

Yes, excessive input is a typical way to produce a buffer overflow.

Andrew Cottrell - *2022-08-18*

The app crashed due to user doing crazy things.

If you can show that there is a security issue then it can be looked at, but if you want to get it fixed then patches are welcome that stop the crash for crazy/stupid/dumb end users.

Just because you overflowed something does NOT mean there is a security issue.

Log in to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101
+1 (858) 454-5900

Resources

Support
Site Documentation
Site Status

Terms Privacy Opt Out Advertise