Rittgasszer Ákos, Z8WK8D

Summary

ITSecTa's computery security homework's parser, has some bugs. Some of them only functional, an other produces chrash.

Vulnerability details

If the .caff file has mistakes, and can not be processed the program will crash. It happens with empty files or files without correct blocks. Functional bug is for example that the parser doesn't process the credit block.

Proof of concept

The easiest way to reproduce the crash, if you make a .caff file wich is empty. Then give it to the parser, as file to parse. Then the parser will crash.

Mitigation

Best solution to fix the crash, if you check the caff container's size. If it's 0, then don't pass it to the create_valid_ciff function (or put the check in the function).