

SatOri Advisory

SATA010410

WinAsm Studio

Summary

A vulnerability has been discovered in WinAsm Studio, which can be exploited by malicious, anonymous individuals to compromise a vulnerable system.

The vulnerability is caused as a result of improper bounds checking when reading *.RC files. This can be exploited to cause a stack-based buffer overflow by tricking a user into opening a maliciously constructed WinAsm project.

Successful exploitation of this vulnerability enables execution of arbitrary code.

