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.

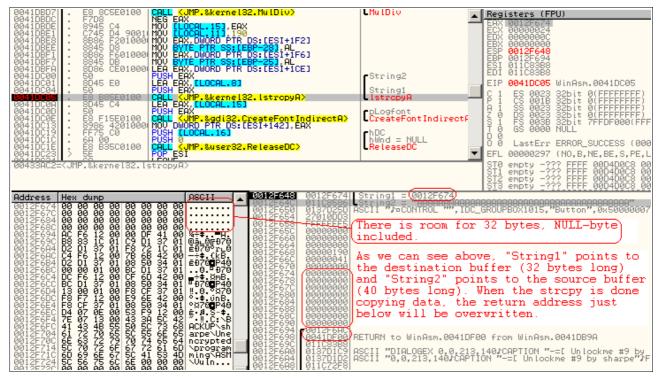
Affected Versions

This vulnerability is confirmed in the following versions:

• WinAsm Studio 5.1.8.0

Other versions may also be affected.

Screen-dumps



Resolution

There is currently no fix for this issue.

Timeline

- Vulnerability identified: 01.04.10
- Vendor informed: 06.04.10
- Vendor fix: Currently unavailable

References

- http://blog.sat0ri.com/?p=481
- http://www.winasm.net/