SatOri Advisory

SATA020110

Crimson Editor

Summary

A vulnerability has been discovered in Crimson Editor, 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 words from dictionary files. This can be exploited to cause a stack-based buffer overflow by tricking a user into using a maliciously constructed dictionary file.

Successful exploitation of this vulnerability enables execution of arbitrary code.

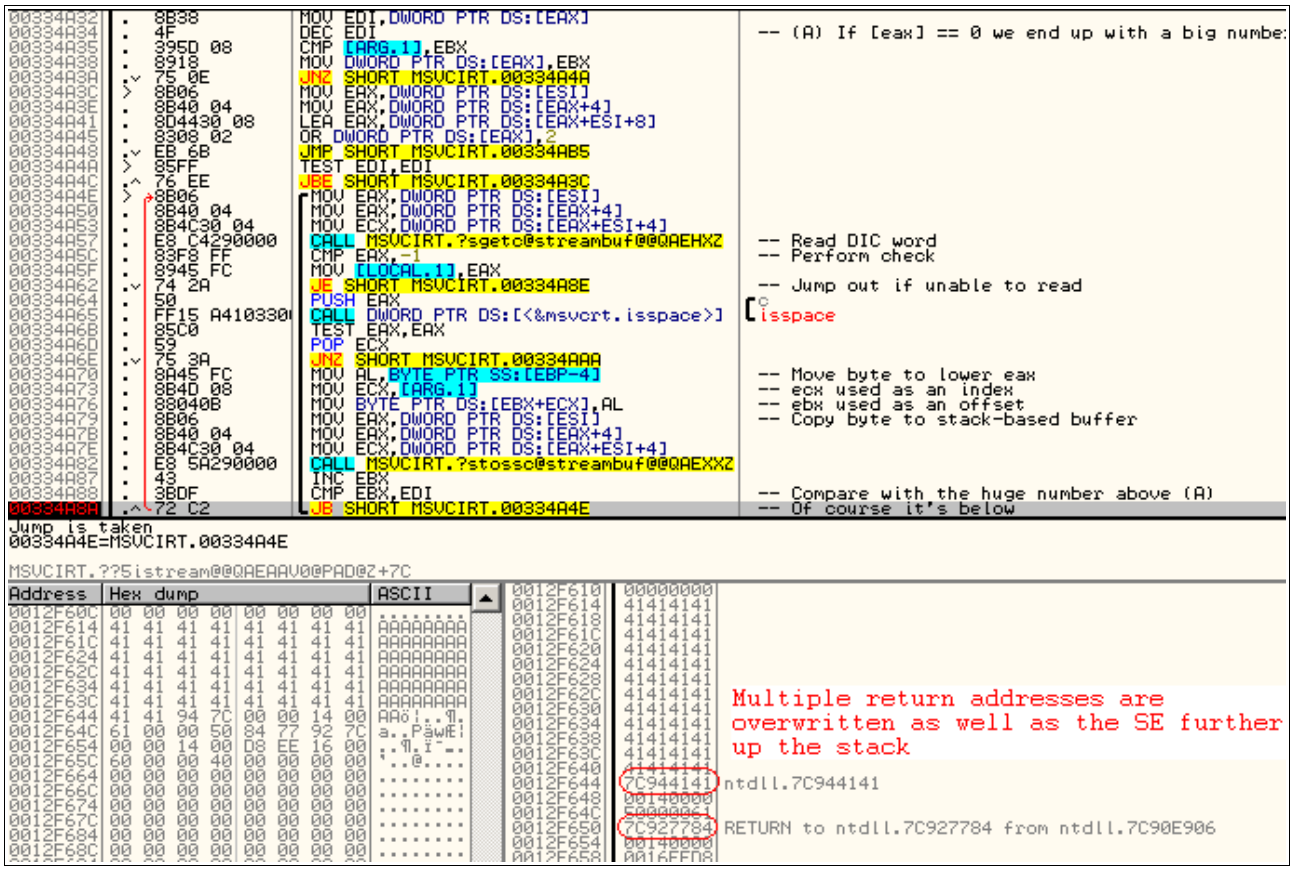
Affected Versions

This vulnerability is confirmed in the following versions:

- Crimson Editor SVN263 English
- Crimson Editor 3.70 Release (Freeware)

Other versions may also be affected.

Screen-dumps



Resolution

Update to Crimson Editor SVN286

Timeline

- Vulnerability identified: 02.01.10
- Vendor informed: 25.03.10
- Vendor fix: 02.04.10

References

- http://blog.sat0ri.com/?p=414
- http://www.crimsoneditor.com/
- http://forum.emeraldeditor.com/index.php?topic=361.0