

# Understanding Heap Overflow Exploits

Jack Koziol of Shellcoder's Handbook fame spoke at ChicagoCon last year on heap overflow exploitation, so we thought we'd share the entire audio recording and slide deck with you as an example of the type of talks you'll see at the next ChicagoCon in May 2009.

As defined by Wikipedia, "A heap overflow is a type of buffer overflow that occurs in the heap data area. Like all buffer overflows, a heap overflow may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain. A routine is vulnerable to exploitation if it copies data to a buffer without first verifying that the source will fit into the destination. A deliberate exploit may result in data at a specific location being altered in an arbitrary way, or in arbitrary code being executed."

So what does all that mean and how do you do it? Find out in Jack's talk on "the most common type of heap overflow exploits for Linux and Windows. He will briefly explain how dynamically allocated memory works, its interaction with the heap memory structure, and how a normal heap operates. Jack will then demonstrate how heap overflows occur, and how they can be exploited on Linux, Windows 2000 and Windows XP SP2 with Data Execution Prevention (DEP) enabled. Unfortunately, the Vista portion of the talk had to be withdrawn. Expect to laugh, cry, and be entertained!"

[del.icio.us](http://del.icio.us)

Discuss in Forums {mos\_smf\_discuss:/root}

Jack Koziol is with InfoSec Institute in Chicago and will also be instructing CEPT, Certified Expert Penetration Tester, at ChicagoCon 2009s from May 4 - 8. For more details, [Click HERE!!](#)

Below are the media files associated with the talk and are available for free downloading:

MP3

Time: 44:43

File Size: 16.1 MB

## Slide Deck

Slides: 21

File Size: 347 KB

Jack Koziol is a Senior Instructor and Security Program Manager at InfoSec Institute and a provider of advanced ethical hacking training. He regularly is called upon to train members of the United States intelligence community, military, and federal law enforcement agencies. Additionally, Jack provides training for Fortune 500 companies, such as Microsoft, HP and Citibank on how to better secure their networks and applications. Jack has appeared in USA Today, CNN, MSNBC, First Business and other media outlets for his expert opinions on information security. Jack is the lead author of The Shellcoder's Handbook.