

Exploiting .ANI

timeline

- Mar 28th (Wed) McAfee contacts MS
- Mar 29th (Thu) Microsoft releases advisory
- Mar 30th (Fri) Public attacks increase
- Mar 30th (Fri) Metasploit module released!
- Mar 31th (Sat) Metasploit supports Vista :-)

timeline

- Apr 1st (Sun) MS announces early release
- Apr 2nd (Mon) Metasploit supports SMTP
- Apr 3rd (Tue) MS releases MS07-017 patch

vuln highlights

- Stack overflow not affected by /GS
- ASLR bypassed via partial overwrite
- RIFF format provides room to play
- Exploit via IE, Outlook, Firefox
- Exception is caught by the library

exploit details

- Randomized RIFF chunks and data
- Use a partial address overwrite for Vista
- Attempt multiple ANI files sequentially
- Able to deliver via single MIME document