

Contents

1. Info.....	2
2. Discussion.....	2
3. Exploit.....	2
4. Solution.....	3
5. Reference	3



1. Info

VLC Media Player 'ftp://' URI Handler '.xspf' File Buffer Overflow Vulnerability

Bugtraq ID: ???
Class: Boundary Condition Error
CVE: ??
Remote: Yes
Local: Yes
Published: Feb 21 2011 12:00AM
Updated: Feb 21 2011 12:00AM
Credit: ax0us
Vulnerable: VideoLAN VLC media player 0.8.6

Not Vulnerable: VideoLAN VLC media player 1.0
VideoLAN VLC media player 1.0.5
VideoLAN VLC media player 1.1.3
VideoLAN VLC media player 1.1.7

2. Discussion

VLC media player is prone to a buffer overflow vulnerability in “**libaccess_ftp_plugin.dll**” because the application fails to perform adequate boundary checks on user-supplied input.

Attackers may leverage this issue to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

VLC media player 0.8.6 is vulnerable; other versions may also be affected.

3. Exploit

Exploit Code : vlc-d0s-exploit.plx (Attached separately)

Code Credit : ax0us, h3rcul3s



4. Solution

Upgrade to the latest version of VLC media player.

5. Reference

- [VLC Homepage](#) (VideoLAN)

