

11 December 2007

By: Bogdan Popa, Security and Search Engines Editor



Winamp

[Windows Media Player and Winamp Users in Danger!](#)

Due to a 3ivx MPEG-4 5.x vulnerability

Windows Media Player and Winamp, two popular software solutions installed on millions of Windows computers, are vulnerable to attacks due to a 3ivx MPEG-4 5.x glitch reported a few days ago. Because the two programs use the MP4 codec, all the computers that installed Windows Media Player and Winamp could be accessed by anyone who managed to exploit the flaw, security companies warned. According to "The Register", Raymond Ball wrote on the Symantec DeepSight Threat Management System that an exploitation could be conducted through a simple malicious MP4 file. "The exploit works by supplying victims with a maliciously formed MP4 file. When a victim unknowingly clicks a link that appears safe, the MP4 content is delivered, causing the exploit to run", it was mentioned in the message posted on DeepSight Threat Management System. Security company Secunia reported the 3ivx MPEG-4 5.x flaw yesterday, attaching a highly critical level as it might have serious consequences for an affected system. "The vulnerabilities are caused due to boundary errors in 3ivxDSPMediaSplitter.ax when processing certain atoms ('©art', '©nam', '©cmt', '©des', and '©cpy') in MP4 files and can be exploited to cause stack-based buffer overflows via a specially crafted MP4 file", Secunia wrote in the security advisory. You're probably wondering if there's any chance to remain secure when you're using Windows Media Player version 6.4.09.1130, Media Player Classic version 6.4.9.0 or Winamp... Well, it may be a solution to avoid a successful exploitation, although it might sound a little bit extreme: "remove the codec or disable media players that use the MP4 codec until the hole is plugged", as the Symantec expert noted, according to "The Register". Just like usual, you can download the latest version of Winamp straight from our Windows software section available [here](#).