

- [Webroot® AntiVirus](#) Get Virus and Spyware Protection that won't Hog your PC's Resources [www.Webroot.com.au/AntiVirus](http://www.Webroot.com.au/AntiVirus)
- [The Missing Link - Sydney](#) Network Storage - we service IT systems, but we look after people. [themissinglink.com.au](http://themissinglink.com.au)
- [Anti-Spyware Download](#) Free Spyware & Trojan scan. Winner of Best Anti-Spyware. Rated 5 Stars! [www.pctools.com](http://www.pctools.com)

Ads by Google

Where am I? > Home > News > Bugs & Fixes



Flaw affects versions 5.05 and 5.06

## Hackers exploit critical Winamp flaw

Media player vulnerability could allow execution of arbitrary code

Robert Jaques  
[vnunet.com](http://vnunet.com), 26 Nov 2004

IT security experts have uncovered a critical vulnerability in the popular Winamp media player, which could be exploited by hackers to compromise a user's system.

Security expert Brett Moore, from Security-Assessment.com, published an advisory detailing the flaw. "The vulnerability is caused due to a boundary error in the 'IN\_CDDA.dll' file," it stated.

"This can be exploited in various ways to cause a stack-based buffer overflow, e.g. by tricking a user into visiting a malicious website containing a specially crafted '.m3u' playlist."

Yesterday the threat level of the flaw was raised to 'critical' after the discovery of a hacker exploit which takes advantage of the vulnerability. Successful exploitation allows execution of arbitrary code, said Moore.

The vulnerability has been reported in version 5.05 and confirmed in version 5.06. Prior versions may also be affected, according to Moore, and the flaw has not been fixed in Winamp version 5.06 contrary to vendor statements.

The best workaround for the hundred of thousands of users of the media player is to disassociate '.cda' and '.m3u' extensions from Winamp.

Have your say | Send to a friend | Print | Digg | Reddit | Share

Tags:

**DO YOU AGREE?**

Have your say on this article

**FURTHER READING**

- [Millions at risk from Java Virtual Machine flaw](#)  
Security experts predict imminent exploit
- [Phishers use zombie nets to automate attacks](#)  
Anti-Phishing Working Group reports 'disturbing' new trend
- [Tasin worms ate my Windows files](#)  
Newly intercepted mutants spreading rapidly

Most read | Most commented | Most watched

- Windows Phone 7 can't connect to hidden Wi-Fi networks
- A week in security: experts warn of cyber war threat
- Enterprise turns from Microsoft to Linux
- HTC HD7 coming exclusively to O2
- Government slammed for wasteful IT spending

More comments

**ANALYSIS AND REPORTS**

- [Detect and survive: the impact of forensic software on security](#)  
How to scan and forensically examine your entire network for evidence of malware, rootkits and stolen files.
- [Ensuring high service levels in cloud computing](#)  
This white paper outlines the considerations you need to make as you plan a move to the cloud

**POLL**

**Amazon Kindle and Sony Reader poll**

Do e-book readers have a place in the enterprise?

- Yes, they are useful for reading PDFs and other work documents
- Yes, once they have colour screens as standard
- Maybe, but it depends on storage capacity and cost
- No, firms are better off investing in tablet PCs
- No, they are purely a consumer device

View poll results | Vote

- [Webroot Official AU Store](#) [www.Webroot.com.au](http://www.Webroot.com.au)  
Protect your PC with Award-Winning Security Solutions from Webroot!
- [The Missing Link - Sydney](#) [themissinglink.com.au](http://themissinglink.com.au)  
Network Storage - we service IT systems, but we look after people.
- [Anti-Spyware Download](#) [www.pctools.com](http://www.pctools.com)  
Free Spyware & Trojan scan. Winner of Best Anti-Spyware. Rated 5 Stars!
- [Zerospam New Zealand](#) [www.zerospam.co.nz](http://www.zerospam.co.nz)  
Stops spam, viruses and phishing attacks before they can enter NZ

Ads by Google

White paper library | Latest white papers

- Creating a dynamic infrastructure through virtualization
- The security challenge: why desktop security is irrelevant in the mobile world

Newsletter signup