LATEST NEWS

- Telecom result helped by $27m compensation payment
- Gen-i awarded datacentre contract with Air New Zealand
- FRY UP: They may be watching you
- Five govt agencies engage with Public Records Act
- Telecom revenue down, but some improvement seen
- Australian election… why IT matters

WinAmp blows another security fuse

Latest in a string of serious vulnerabilities

BY MATTHEW BROERSMA | LONDON | THURSDAY, 25 NOVEMBER, 2004

EMAIL PRINT

For those IT managers who've been eagerly anticipating the next major WinAmp security flaw, the wait is over. Brett Moore of Security-Assessment.com this week published details of a security hole allowing attackers to take over a PC when a user visits a specially crafted web page.

The bug, a boundary error in the IN_CDDA.dll file, is the latest in a string of serious vulnerabilities in WinAmp, including an August flaw in the handling of "skin" files which attackers began to exploit before it had been discovered by researchers. The new bug, the skin file flaw and an April flaw in the handling of ".xm" files could all be exploited by luring an affected user to a website containing a specific type of file, which would then be automatically downloaded and executed.

This week's bug can be exploited in a number of ways, the most dangerous being via an ".m3u" playlist file, according to Moore. "When hosted on a website, these files will be automatically downloaded and opened in winamp without any user interaction," he wrote in Security-Assessment.com's advisory. "This is enough to cause the overflow that would allow a malicious playlist to overwrite EIP and execute arbitrary code."

Nullsoft, part of America Online, has patched the bug in WinAmp version 5.06, available from the company's website. Danish security firm Secunia, which maintains a vulnerabilities database, said the bug was "highly critical", its second most serious ranking.

The August vulnerability was WinAmp's most serious this year because it was exploited before a patch was available. While not as widely used as Windows Media Player or RealPlayer, WinAmp has an installed base of several million, including corporate desktops, according to the company. The bug affected version 5.04, which was only a month old at the time.

EMAIL
PRINT
SHARE THIS STORY WITH:

MOST POPULAR

READ | COMMENTED | EMAILED | SHARED

- Netbook failure rate disappoints major user
- Canterbury University signs alliance with Microsoft
- File-sharing bill could extend surveillance culture - Bott
- How to roll out full disk encryption on your PCs and laptops
- Ernie Newman resigns