

# [NT] AOL Nullsoft Winamp Ultravox Lyrics3 v2.00 tags Heap Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-10/msg00100.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Oct 2006 12:06:24 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

AOL Nullsoft Winamp Ultravox Lyrics3 v2.00 tags Heap Overflow

---

## SUMMARY

Lyrics3 is "a system for embedding the lyrics inside an MP3 song file. The Winamp media player has support for this protocol". Remote exploitation of a heap-based buffer overflow vulnerability in the Ultravox Lyrics3 parsing code in AOL Corp.'s Nullsoft Winamp media player could allow an attacker to execute arbitrary code in the context of the currently logged in user.

## DETAILS

### Vulnerable Systems:

- \* Winamp version 5.24
- \* Winamp version 5.3

### Immune Systems:

- \* Winamp version 5.31

Due to an error in the parsing of certain Lyrics3 tags, a malicious server can cause the Winamp client to allocate a very small amount of space and then try fill it with a large amount of server supplied data, potentially overwriting values which will lead to code execution.

Analysis:

Exploitation allows remote attackers to execute code in the context of the user who started Winamp. Exploitation requires that attackers social engineer victims into connecting to a server. This can be accomplished by embedding a link in a web page to a playlist file, a 'shout:' URI or a 'uvox:' URI, which are automatically loaded by Winamp from Internet Explorer. Alternatively, one of these items could be placed in a playlist file. However, attackers cannot force users to open the content they have supplied.

Disclosure Timeline:

- 10/19/2006 – Initial vendor notification
- 10/25/2006 – Initial vendor response
- 10/25/2006 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@xxxxxxxxxxxxx>> iDefense Labs Security Advisories.  
The original article can be found at:  
<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=432>>  
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=432>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.