

# Re: Winamp: Mp3 file can control the minibrowser

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0064.html>

**From:** Security ([Security@gracernote.com](mailto:Security@gracernote.com))

**Date:** 04/04/02

Date: Wed, 03 Apr 2002 14:49:07 -0800

From: "Security" <[Security@gracernote.com](mailto:Security@gracernote.com)>

To: "Andreas Sandblad" <[sandblad@acc.umu.se](mailto:sandblad@acc.umu.se)>, [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

Thank you for your posting of a Cross-Site Scripting issue with the mini-browser that is included with WinAmp 2.78 and above. Gracernote supplies the underlying technology for the mini-browser. We have fixed the encoding issue at the server. Should you find any additional security issues with the mini-browser, please send email to [security@gracernote.com](mailto:security@gracernote.com).

Thanks to Andreas Sandblad for bringing this to our attention.

Matthew Leeds  
VP Operations  
Gracernote  
[www.gracernote.com](http://www.gracernote.com)

\*\*\*\*\* REPLY SEPARATOR \*\*\*\*\*

On 4/3/2002 at 1:23 PM Andreas Sandblad wrote:

```

>=====
>Title: Winamp: Mp3 file can control the minibrowser
>Date: [2002-04-3]
>Tested env: Winamp 2.78c, 2.79 with Win2000 Pro
>Impact: A special crafted mp3 file can control the
> minibrowser, such as directing to arbitrary
> webpage possibly containing malicious
> html code. Also another "call home" issue.
>Status: Winamp contacted over two weeks ago,
> no response.
>Vendor fix: Non. The fix should be on the server side.
>Workaround: Disable minibrowser. __
> (enabled by default) o' \, =./ `o
>Author: Andreas Sandblad, sandblad@acc.umu.se (o o)
>-----ooO--( )--Ooo--
>
>PROBLEM:
>Winamp has a built-in minibrowser to show information about songs beeing
>played (enabled by default). For every song currently playing Winamp will
>direct the minibrowser to an url like

```

SecurityFocus Bugtraq: Re: Winamp: Mp3 file can control the minibrowser

><http://info.winamp.com/winamp/WA.html?Alb=Project&Cid=winamp&Tid=&Track=Brick>  
>Winamp gets the title/artist/album information from the ID3v1/ID3v2 tag in the mp3 file. The problem is that the html page doesn't filter "<" and ">" characters making it possible to inject htmlcode to control the minibrowser (yet another CSS problem).  
>  
>EXPLOIT:  
>Every field in the ID3v1 tag is limited to max. 32 bytes so we use the ID3v2 tag instead. It seems that Winamp has made some useless efforts to stop our attack, namely to convert " and ' to \" and \' (server side).  
>This will of course not stop us.  
>  
>So lets put the following html code in the album field of the ID3v2 tag of our mp3-file:  
><mp3 id=m src=<http://ANYURL>><script>location=m.src</script>  
>It will direct the user to <http://ANYURL> on load.  
>  
>Adding an ID3v2 tag to a mp3 file is very simple. Open the file in Winamp, right click on it and choose "File info". Unmark the ID3v1 tag and mark ID3v2. Add the html code in the album field. Sometimes Winamp will complain when creating the ID3v2 tag with some characters. Then you simply have to hexedit the mp3 file instead.  
>  
> \_ \_  
> o' \, =, / `o  
> (o o)  
>-----ooO--( )--Ooo--  
>Andreas Sandblad, student in Engineering Physics  
>at the University of Umea, Sweden.  
>-----

- 
- **Previous message:** [Georgi Guninski: "More Office XP problems \(Version 2.0\)"](#)
  - **In reply to:** [Andreas Sandblad: "Winamp: Mp3 file can control the minibrowser"](#)
  - **Next in thread:** [Daniel Lorch: "Re: Winamp: Mp3 file can control the minibrowser"](#)
  - **Next in thread:** [Andreas Sandblad: "Re: Winamp: Mp3 file can control the minibrowser"](#)
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)