

# [NT] Unchecked Buffer in Windows Shell Could Enable System Compromise

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0060.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 12/19/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 19 Dec 2002 18:03:54 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Unchecked Buffer in Windows Shell Could Enable System Compromise

---

## SUMMARY

The Windows Shell is responsible for providing the basic framework of the Windows user interface experience. It is most familiar to users as the Windows Desktop, but also provides a variety of other functions to help define the user's computing session, including organizing files and folders, and providing the means to start applications.

An unchecked buffer exists in one of the functions used by the Windows Shell to extract custom attribute information from audio files. A security vulnerability results because it is possible for a malicious user to mount a buffer overrun attack and attempt to exploit this flaw.

An attacker could seek to exploit this vulnerability by creating an .MP3 or .WMA file that contained a corrupt custom attribute and then host it on a website, on a network share, or send it via an HTML email. If a user were to hover his or her mouse pointer over the icon for the file (either on a web page or on the local disk), or open the shared folder where the file was stored, the vulnerable code would be invoked. An HTML email could cause the vulnerable code to be invoked when a user opened or previewed the email. A successful attack could have the effect of either causing the Windows Shell to fail, or causing an attacker's code to