

[NT] Oddsock Playlist Generator Multiple BufferOverflow vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0099.html>

From: support@securiteam.com

Date: 07/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 22 Jul 2002 22:40:42 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Oddsock Playlist Generator Multiple BufferOverflow vulnerability

SUMMARY

Oddsock Playlist generator is used by Radio DJs to allow listeners to choose a song to play from the Winamp Playlist. Song Requester version 2.1 contains multiple buffer overflows, which will result in a DoS attack against the Winamp/Shoutcast service. The DJ will have to restart Winamp in order to make it work again.

There are two major kinds of DoS attacks against this software: the first will displays an error message, and informs the user that a log file has been created. The second attack closes down Winamp and restores the playlist from the previous state, so that any newly added songs will not be displayed in the playlist. It also restores the administrator password to what it was before it was changed (without restarting Winamp).

DETAILS

Vulnerable systems:

* Song Requester version 2.1

Technical details:

By parsing long names or characters to the CGI files in the Song

