

[NT] Plain Text Password Vulnerability in Winamp

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0086.html>

From: support@securiteam.com

Date: 05/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 21 May 2002 08:49:31 +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.

Plain Text Password Vulnerability in Winamp

SUMMARY

Winamp is a popular MP3 and other Audio codec's listening program, the program has been found to contain a security vulnerability that would allow a local attacker to gain username and password used for streaming (and possibly used elsewhere) by reading Winamp's configuration file.

DETAILS

Vulnerable systems:

- * Winamp version 2.80

When a URL's is streamed in Winamp that requires HTTP authentication, the user is prompted to enter a username and password. This username and password is then stored as plain text in the file winamp.ini under the section [HTTP-AUTH]. The format of stored passwords (it seems) is <domain - TLD>=<username>:<password>.

URL's that are streamed are also kept as history in the winamp.ini file under the [winamp] section. This includes URL's which include the username/password in them (i.e. <http://username:password@site>).

ADDITIONAL INFORMATION

Securiteam: [NT] Plain Text Password Vulnerability in Winamp

The information has been provided by <mailto:isox@chainsawbeer.com> isox.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Stronghold Secure Webserver Sample Script Path Disclosure Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)