

[UNIX] Default Installation Insecurity in MS WMP for Sparc/Solaris

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0086.html>

From: support@securiteam.com

Date: 10/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: 19 Oct 2002 04:33:16 +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

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.

Default Installation Insecurity in MS WMP for Sparc/Solaris

SUMMARY

Microsoft Windows Media Player v6.3 for Sparc/Solaris is available for download from <http://download.microsoft.com>

<http://download.microsoft.com>. A security vulnerability in the installer causes the product to install the binary files of the product in an insecure manner.

DETAILS

When you install Microsoft Windows Media Player on a Solaris machine (the program is distributed as an executable installer that takes care of everything), the executables are installed as word-writable files, effectively ignoring the umask of the installer.

It means that anybody with an account on the system can change those executables and put a Trojan in them. People executing the program later will happily run the Trojan and have their account compromised.

ADDITIONAL INFORMATION

The information has been provided by <mailto:sam@rfc1149.net> Samuel Tardieu.

Securiteam: [UNIX] Default Installation Insecurity in MS WMP for Sparc/Solaris

=====
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: "[REVS] Chrooting Daemons and System Processes HOW-TO"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)