

[NEWS] AIM Filter Contains Spyware and Backdoors

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0028.html>

From: support@securiteam.com

Date: 01/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 8 Jan 2002 23:31:02 +0100 (CET)

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.

AIM Filter Contains Spyware and Backdoors

SUMMARY

<<http://www.securiteam.com/tools/5CP050U61M.html>> AIM Filter contains spyware and backdoors in its official release. The w00w00 group has been kind enough to provide a clean version of the product.

DETAILS

The w00w00 group has announced that AIM Filter, a solution to the AIM buffer overflow vulnerability, actually contains backdoors and spyware. This became obvious when the source was released on January 5th, 2002.

At the time, Robbie Saunders' AIM Filter seemed like a nice temporary solution. Unfortunately, it instead produces cash-paid click-through over time intervals and contains backdoor code combined with basic obfuscation to divulge system information and launch several web browsers to porn sites. The w00w00 group only took the time to verify that it blocked the attack, since an analysis of AIM filter was not our priority.

In the meantime, w00w00 has cleaned up the AIM Filter code and produced a modified version available on their website, and they have removed all the backdoors and spyware. For those of you who are still interested in using

Securiteam: [NEWS] AIM Filter Contains Spyware and Backdoors

the software, we strongly recommend you use this modified version instead.

You will find it at:

<<http://www.w00w00.org/files/w00aimfilter.zip>>

<http://www.w00w00.org/files/w00aimfilter.zip>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jpr5@darkridge.com>> Jordan Ritter of w00w00.

=====

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: "[NT] Hosting Controller Multiple Security Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)