

[NT] Privilege Escalation Flaw in AClient Service for Windows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/22/04

To: list@securiteam.com

Date: 22 Nov 2004 11:38:06 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Privilege Escalation Flaw in AClient Service for Windows

SUMMARY

A privilege escalation technique can be used to gain SYSTEM level access while interacting with the AClient Service for Windows tray icon.

DETAILS

Vulnerable Systems:

- * AClient Service for Windows version 5.6.181
- * Altiris Deployment Solution 5.6 SP1 (Hotfix E)

Exploit:

1. Right click on the Altiris Client Service icon in the Taskbar and choose View Log File
2. Notepad should open. Click File, click Open
3. In the Files of type: field choose All Files
4. Navigate to %WINDIR%\System32\
5. Right click on cmd.exe and choose Open
6. A new command shell with launch with SYSTEM privileges

ADDITIONAL INFORMATION

Securiteam: [NT] Privilege Escalation Flaw in AClient Service for Windows

The information has been provided by <mailto:reedarvin@gmail.com> Reed Arvin.

=====

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.