

# [NT] Altiris Deployment Server Design Flaw

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0142.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/26/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 26 May 2005 17:55:41 +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>

-----

Altiris Deployment Server Design Flaw

---

## SUMMARY

<<http://www.altiris.com/products/deploymentsol/#ss>> Altiris Deployment Server provides remote control solution over client machines. A design flaw in the Deployment Server architecture that allows attackers to take complete control over all Altiris clients on a network with relative ease.

## DETAILS

Vulnerable Systems:

\* Altiris Deployment Server – 5.x, 6.x

The flaw is that the AClient.exe process does not request any authentication from the Deployment server and will happily connect to any Deployment server it finds and give it complete Administrator rights to the machine along with the ability to Remotely Control it. This flaw can be exploited via physical or wireless access to the network Deployment Server is on, or remotely through a compromised system anywhere on the network that Altiris Deployment server is on and can potentially give an attacker complete administrative access to some or all managed clients. This can be done with little or no advance knowledge of the network or client configurations prior to the attack, depending on the AClient.exe configuration used.

## Securiteam: [NT] Altiris Deployment Server Design Flaw

### Solution:

Due to a design flaw in the AClient.exe's lack of a proper authentication system, there is little you can do to prevent these exploits.

The best things you can do to protect yourself until Altiris fixes their product is:

1) Do not use the "Use TCP/IP Multicast to locate a Deployment Server" option when installing ACLIENT.EXE.

Setting in a fixed IP address and Port number when installing the client will make it more difficult for someone to exploit this flaw. An attacker will have to disable the existing deployment server first, or use some other trick to make the attacker's machine seem like the "real" Deployment server.

2) Turn on the "Encrypt Sessions with Server" and the "Require Encrypted Sessions with Server" option when installing ACLIENT.EXE

This will require a client computer to reboot before it can be compromised, which creates an additional barrier of entry to an attacker, and give you more time to react in the event a Rogue Deployment server is detected on the network.

3) Turn on the "Remain Connected to the server" option when installing ACLIENT.EXE.

This will provide less of an opportunity for a client to unknowingly connect to a Rogue Deployment Server by maintaining the connection to the one the client first connected to.

4) Do not use the "Advertise the server this client is connected to through multicasting" option unless absolutely required.

This would prevent a rouge deployment server from obtaining an additional compromise vector (the advertising AClient.exe connected to a rogue DS) to new machines to control.

### Exploits:

#### Prerequisite:

BadGuy gets access to the network either (1) physically, by walking in the door and plugs his laptop into any network jack anywhere in the building or connecting to a wireless network access point inside or outside of the building, or (2) by gaining access to any computer on the network, such as through any variety of cracks, viruses, Trojans, stolen password, etc..

For purposes of this discussion, we will assume that he simply walks in the door and plugs in a network cable, though it really makes no difference how he connects in order to exploit this flaw.

Scenario I: AClient.exe configured to connect to Deployment Server via network broadcast:

The attacker's laptop is running its own copy of Deployment Server ("DS" from here on) (which is available for a free download online (though it is limited to 10 clients)). When clients are booted up, they will send a broadcast request to the network. If the laptop responds faster than the company's "Official" DS ("ODS" from here on) , then the client will

## Securiteam: [NT] Altiris Deployment Server Design Flaw

connect to it, and BadGuy now has complete control over the client through the AClient service.

Furthermore, if BadGuy can knock the official DS off the network (through any variety of Denial of Service attacks, ARP Poisoning, etc.) it can assume the role of the ODS, with the same IP address even, and take over more clients. Additionally BadGuy can potentially determine the IP address of the ODS by watching network traffic and seeing the broadcast messages that are sent to the ODS, in order to determine the IP address to attack and assume the role of.

Scenario II: AClient.exe configured to connect to Deployment Server via direct IP address (for example, IP: 1.2.3.4) or hostname:

Same as above, but BadGuy can redirect clients to his laptop by ARP-Poisoning (which makes the network's switches and routers think that the laptop is the machine they should send connect to for the IP address 1.2.3.4) or by using a Denial of Service attack to knock the ODS offline, and the laptop then starts functioning with the IP address 1.2.3.4. Again, complete control of all clients is on the network is easily achieved.

Scenario III: AClient.exe configured to connect to Deployment Server via encrypted connection:

Same as above scenarios except that it will require that a client to reboot (for any reason) before the client can be hijacked. When the client computer reboots, it will request new session keys from the DS, in this case the BadGuy's DS, and will use these keys (now provided by BadGuy's DS) to encrypt the session communications.

Vendor Status:

Altiris tech support was notified of this problem and sent the details of this vulnerability on Friday, November 21, 2003. Altiris confirmed the problem and assigned it to a support ticket which was escalated for management attention. The author was informed that it had been scheduled to be fixed in a future release, but they did not provide an ETA or any other details. Since then no follow-up inquiries to Altiris have been responded to. Since it has been nearly a year, with three new versions (6.0, 6.1, 6.1sp1) and it still does not appear to have been resolved, the author published this alert to inform systems administrators of the vulnerability to their networks.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:bugtraq@diamondsea.com> rian Gallagher.

=====

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

Securiteam: [NT] Altiris Deployment Server Design Flaw

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