

MWR InfoSecurity Security  
Advisory

Symantec's Altiris  
Deployment Solution –  
ACIntUsr Local Privilege  
Escalation

7<sup>th</sup> January 2010



## Contents

<b>1</b>	<b>Detailed Vulnerability Description .....</b>	<b>4</b>
1.1	Introduction .....	4
1.2	Technical Background.....	4
1.3	Vulnerability Details.....	4
1.4	Exploit Information .....	5
1.5	Dependencies .....	5
<b>2</b>	<b>Recommendations.....</b>	<b>6</b>
<b>3</b>	<b>Further Information .....</b>	<b>6</b>
<b>4</b>	<b>References.....</b>	<b>7</b>

## Affected Software Vulnerability Type

<b>Package Name:</b>	Symantec's Altiris Deployment Solution
<b>Date:</b>	2009-10-07
<b>Affected Versions:</b>	Version prior to 6.9 SP3

<b>CVE Reference</b>	CVE-2009-3108
<b>Author</b>	L. Jennings
<b>Severity</b>	High
<b>Local/Remote</b>	Local
<b>Vulnerability Class</b>	File ACL misconfiguration
<b>Impact</b>	A local user of a system on which the Altiris agent was installed could Trojan an autorun binary and so gain access to the account of any user who logged onto the system.
<b>Vendor Response</b>	The vendor has addressed the issue in a new Service Pack
<b>Exploit Details Included</b>	Yes
<b>Affected OS</b>	Microsoft Windows

### Overview:

A vulnerability has been identified in the autorun ACIntUsr.exe binary installed as part of the Altiris software agent on managed clients. It was found to allow write access to any user.

### Impact:

A local attacker could replace or infect the binary with malicious code that would then run automatically every time a user logged in. Any malicious code would run with the privileges of the targeted user account.

### Cause:

An overly permissive ACL is applied to the executable file.

### Interim Workaround:

Manually modify the ACL on the file to prevent write access to general users.

### Solution:

It is recommended that users upgrade to the latest Service Pack.

[http://www.symantec.com/business/security\\_response/securityupdates/detail.jsp?fid=security\\_advisory&pvid=security\\_advisory&suid=20090826\\_00](http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20090826_00)

## 1 Detailed Vulnerability Description

### 1.1 Introduction

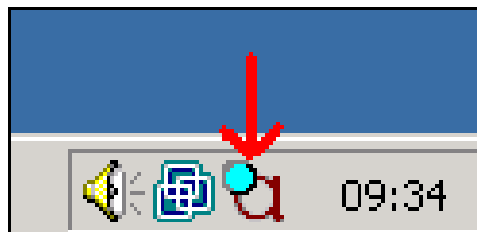
*“Altiris Deployment Solution 6.9 software helps reduce the cost of deploying and managing servers, desktops, notebooks, and thin clients from a centralized location in your environment. An easy-to-use, automated deployment solution offers OS deployment, configuration, PC “personality” migration, and software deployment across hardware platforms and OS types, including Microsoft Windows 7 and Windows Server 2008 R2.” – Symantec Website*

### 1.2 Technical Background

One of the executables that is installed on Altiris managed clients (ACIntUsr.exe), is automatically executed whenever a user logs in; ACIntUsr.exe executes under the privileges of the logged in user. This file is located at the following location by default:

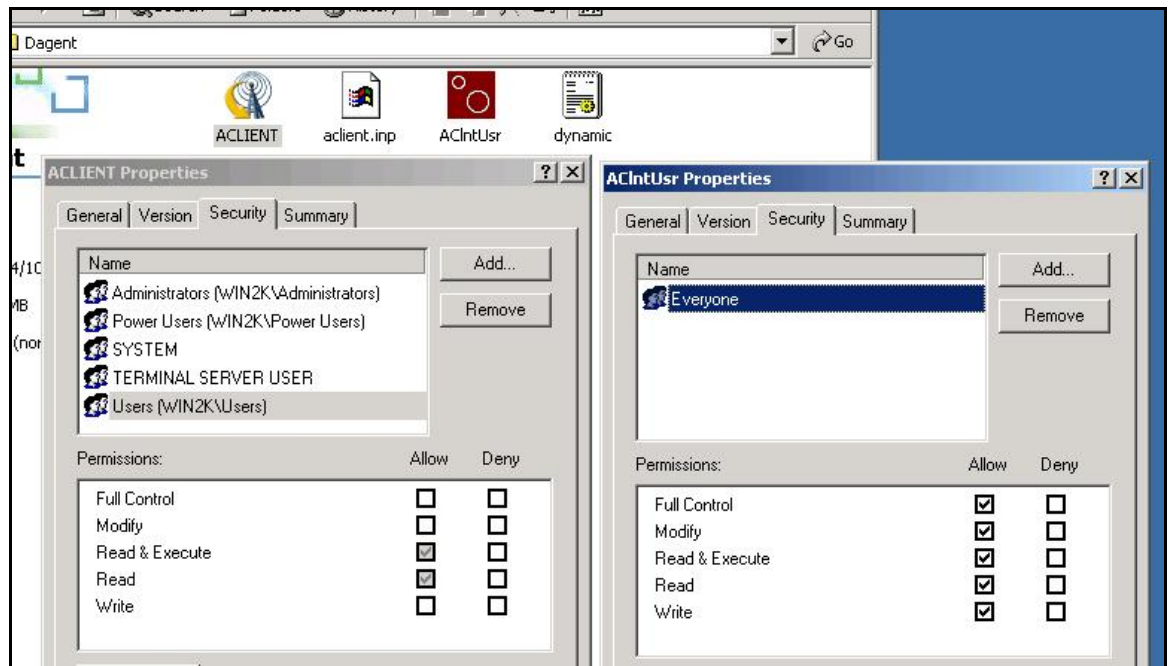
C:\program files\altiris\dagent\acIntusr.exe

This binary represents the GUI control applet for the ACLIENT.exe service and can be seen running in the taskbar when a user logs in: -



### 1.3 Vulnerability Details

Although the ACLs applied to the containing directory and the ACLIENT.exe service binary are secure, the ACL applied to ACIntUsr.exe specifically is insecure in that it allows write access to the EVERYONE group, as can be seen below: -



#### 1.4 Exploit Information

This ACL can be abused to replace this binary with malicious code which will be execute under the security context of the user every time they log in. Consequently, this represents a local privilege escalation issue. However, if users login with domain accounts then this could result in a much wider level of access being obtained. For example, if this were installed on a Terminal Server and then a Domain Administrator logged in to manage the server then this could result in a local unprivileged user gaining domain administrator privileges.

#### 1.5 Dependencies

An attacker would require local access to an Altiris managed client to exploit this issue.

## 2 Recommendations

It is recommended that users should upgrade to the latest Service Pack [1] and ensure that the new software agent is installed on all clients. If this cannot be achieved then the ACL on this file should be manually modified on all clients such that general user accounts are only permitted read access.

## 3 Further Information

For further information on the wider security implications of deployment solutions and Symantec's Altiris Deployment Solution in particular, please refer to the slides from the author's DeepSec '09 presentation at the following location: -

[http://labs.mwrinfosecurity.com/files/Publications/mwri\\_deepsec09\\_weapons-of-mass-pwnage\\_2009-11-20.pdf](http://labs.mwrinfosecurity.com/files/Publications/mwri_deepsec09_weapons-of-mass-pwnage_2009-11-20.pdf)

## 4 References

[1] Altiris Patch Information

[http://www.symantec.com/business/security\\_response/securityupdates/detail.jsp?fid=security\\_advisory&pvid=security\\_advisory&suid=20090826\\_00](http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20090826_00)

MWR InfoSecurity  
St. Clement House  
1-3 Alencon Link  
Basingstoke, RG21 7SB  
Tel: +44 (0)1256 300920  
Fax: +44 (0)1256 844083  
[mwrinfosecurity.com](http://mwrinfosecurity.com)