

MWR InfoSecurity Security
Advisory

Symantec's Altiris
Deployment Solution –
Client/Server Authentication
Bypass

7th January 2010

MWR  INFOSECURITY

Contents

1	Detailed Vulnerability Description	4
1.1	Introduction	4
1.2	Technical Background.....	4
1.3	Vulnerability Details.....	5
1.4	Exploit Information	5
1.5	Threat Scenarios.....	6
1.5.1	External Attacks – Mobile Devices	6
1.5.2	Internal Attacks – Intercepting Internal Communications	6
1.6	Dependencies	8
2	Recommendations.....	9
3	Further Information	9
4	References.....	10

Affected Software Vulnerability Type

Package Name:	Symantec's Altiris Deployment Solution
Date:	2010-01-07
Affected Versions:	Versions prior to 6.9 SP3

CVE Reference	CVE-2009-3109
Author	L. Jennings
Severity	High
Local/Remote	Remote (requires intercepted communication from a client)
Vulnerability Class	Logic Flaw
Impact	Complete administrative control of the client
Vendor Response	The vendor has addressed the issue in a new Service Pack
Exploit Details Included	Yes
Affected OS	Microsoft Windows

Overview:

A vulnerability has been identified in the software agent in the client that connects to the deployment server. It does not properly track the current authentication status of the server to which it connects and so can be tricked into accepting commands without verifying the authenticity of the server.

Impact:

Full administrative control over the client can be gained by an attacker able to intercept the communication from a client directed towards the deployment server.

Cause:

The agent does not check the state of its authentication with the server when receiving commands, meaning that a malicious server which did not use the protocol in the intended manner could issue commands without authenticating itself to the client.

Interim Workaround:

Use IPSec or another secure tunnel in order to strongly authenticate and encrypt the communications between software agents and the deployment server on TCP port 402.

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

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

Altiris Deployment Solution manages the clients for which it is responsible by the use of a software agent installed on each client. This agent connects to the deployment server on TCP port 402 (by default). A proprietary ASCII based protocol is then used to update the server with status information about the client and for the client to receive commands from the server.

In order to facilitate secure communication, it is possible to use key-based authentication of the server and encryption of the communication channel. This is intended to allow the software agent on each client to verify the authenticity of the deployment server they are speaking to, and to protect the confidentiality and integrity of the communications.

An example of this authentication and encryption mechanism in action can be seen by viewing the packet dump below. The red traffic is the client and the blue traffic is the server: -

```
Stream Content
Request=Authenticate
CipherText=RwIb\Hq[c`NyyQFRZLINEORxAMHRJUP{FAN`JRIAahjo{g\}ofANTZxw{wncj{tIwzdjqKc}bHeI
[sednKx{ASITen}j-MEMUIEnZ.MvQvdiY^jDE_.dsFnIm}y{keZyB.}NG@ov{obpass\w{udam-x._opp-u
{APgafvopI^hgduYr~}gaoBvThD}v{ousZURQMart|f{bvYebHam_Q}hnr|NIZ.vntSHJZ.cwU}xoIkPRRL}xAMUaP{A}
IF~{xofiedAs{skfgKrI_vapEMqvTppb1TyRpxiBt\FjPIjpuKo@LSE]}_yaoSarwm@syIFc\]}~H
{NCiPHZemosyrXRjIcbdh}\tawyu_AApoKsMdqnhp.bBRUTlIaIKg.lke-w{ackZVqST[C]qCFEzP\G}k@xxNZtn|
BIRMWYnmIDwF|PyvHIqu~euosARGufPrLORAR.NBRHeIDMTtyzZCJfQD-OA`[g]}pyTONUTsHMjLSJM|svqL}
_LTyqHFwTpzT_oxhLrj|VYtwG`l{ngxPw~fvivAC_{mwnpALAV`.iK.Hwx`xBNNCULeuJdsOPTXrw`vrOnZ}yoy}vm}
InYHuoitt|Mn`J.~E@e.Y}\GTWZJm.kuqAPwexAEHVbjFFaNoCUEAYKZtceVkjFF`@U{CAE|bozn}BdP
.Reply=Authenticate
CipherText=QvvcIOJEza`NnkFSAZLYnKhrxyBLUyut{OTopPQ}qr[.}okr\j\cTMM[.]{wyg}jrlwzBkcjcgblu.
[gpw]_Jj\FGwwo`ml\WM^YHlj-MlQrP.}JkDE_iPcsnlq\}|kE|i[Zn[wENTHnhckwDxjCugya`.K}esjh
{QqssvwiH}gtwAb..e~nqdu|IvBZY@qNKWM\cctxmigRIEbxwol@}huw-MIZygEpBON}mFwEX.mIZLqfH\i_OPaPKPT|
G~|xAv.pdzNE{AfU}`ik{pn`hd~Pa~}|@apdg{E`RFjPHnwUIo@N@S_x_y}ngbrGas\}|UryGhAn}QodCZcMYC
\FN@jxsp@|I\TqG}|OAAqQ.QMT`.tu|BusGbmXw{JekdxtqciDY@ZfxwP[U]qsvMHa\InejxJUC.ySMQ|wy_]UsR|
MvrDxvQmeu.qSfbtFPrMH}ArgEFNceyD|C}|fJFFdpDk@ZqAa_]ecGNzutsd_hHGJM|oAt\}_wyYFSDsoEKfxxEu|
koboai`x{yk|@w~va}snB_{mf|gTLXee~wk{FsmannX_JE\`svewJR@unxm|exrocoj}|{Y}Fu.z.YHqohwt|
ywf^arwqroxiJDSGJ\akgnIDTux\EYwrjFveFvbUEZYDjtGfQtkGbd@E}POchckigpz@Aup~aFhhzDDC\iz
[kFHFxi]mhtwokXUT`TAG`RMABbqgpCUZvcUjFcs\O[se~{^YUCEGA`VI`vud.A{drce~YD}|znbswAP
Result=Success
.Request=CreateSession
Session-Key=.....
New-Encryption=Yes
.Reply=CreateSession
Result=Success
.....
```

1.3 Vulnerability Details

The code implementing this in the software agent does not properly track the authentication status. Instead, a simple switch statement is used to process each message type within the protocol when it is received. Consequently, it is possible for a malicious deployment server which does use the protocol in the intended manner to issue commands to the software agent without authentication. This can be achieved by ignoring the authentication challenge and encryption request from the client and issuing alternative commands.

1.4 Exploit Information

An excerpt of a packet dump from a malicious server coded in Python exploiting this issue can be seen below: -

```
Stream Content
Request=SendFile
Filename="c:\mwrtest1234.exe"
Date=1207643970
Attributes=32
Size=115712
Port=6666
Schedule-ID=100000008
Task-Sequence-ID=0
Task-Type=CopyFile
Allow-Defer=5
CurrentFilecount=1
TotalFileCount=1
TotalFileCopsySize=115712
ID=5000001
. Request=Authenticate
CipherText=GuzsLH_DAv`Zy|sfdZLYyKYCxa[IQIU.P.RVK~LAXSgmzoz.gMnys@HIKz`{sodj{u1wzPyyu_cg.Mux
[gsPj_M{}BGE|Kmlc\WMAXUNz0JtQvTikoIDE_nwprnuay{jkAlx_nohUA[SA.f{!sPLE~dAu|`a.koeC{e
{Q@b`vvt}hH{qPf\vn{g}nFwAifTBzGGg_CEWYnetxkebrHEBxamZQ}hovI[IN~hopCJHjObFDLji]}
BRFLxm_KSaPI@.YI~|xxpngd@x@tofq[csJrpsaAgv@wvj]Uw|PxIUUUFjPX|sAMo@LF@Y_asj@frGcTA|
yAvMvz^zo_xUG`pLMqzrF@jxruc|J\tqjixkAAQq{RMTZ}ipp_fvQfzi{YQdw.max}|eAPZRxfvZAlqCTEY`
\MnJzXNT@jYTRYLo^XJH}Fe\bg@ztQreuoCC@vFPrJNSAr.KB_@eiI|C|rBBatba~U@dhgILcpo^A\UTcmAoLSJM|
[VrL]_VvAFwGFha_qomLcmN~@xptA}mr~H|@r~vfnkow_{}GnhPLXsdv.k{it`KD__CPIEdmtBKACQxw|]
vvr_ako|Y|fn|ZoyKpogtT|NaqKmsRQf.H\]SUSOL|n|qA@FeIIO\GpjFvpwowUEYY
[NtwSSbzTgbPAZANP.g.`wAoBp
. Reply=SendFile
Schedule-ID=100000008
Task-Sequence-ID=0
Result=Success
Status-Code=0
Status-Module=AClient
. Request=LiveEvent
Event=Execute
```

As illustrated above, a malicious server could use functionality within the protocol to initiate a file transfer request. In this case this was used to transfer a Metasploit Meterpreter [1] executable to the client system named “mwrtest1234.exe”. It can be seen that this was successful due to the successful reply to the “SendFile” request later in the packet dump.

In the full exploit, a command was then issued to execute this newly transferred file in order to get a reverse connect shell. The software agent runs with SYSTEM level privileges and so full control of the client was obtained.

1.5 Threat Scenarios

This vulnerability presents two main threat scenarios, which will be briefly discussed below.

1.5.1 External Attacks – Mobile Devices

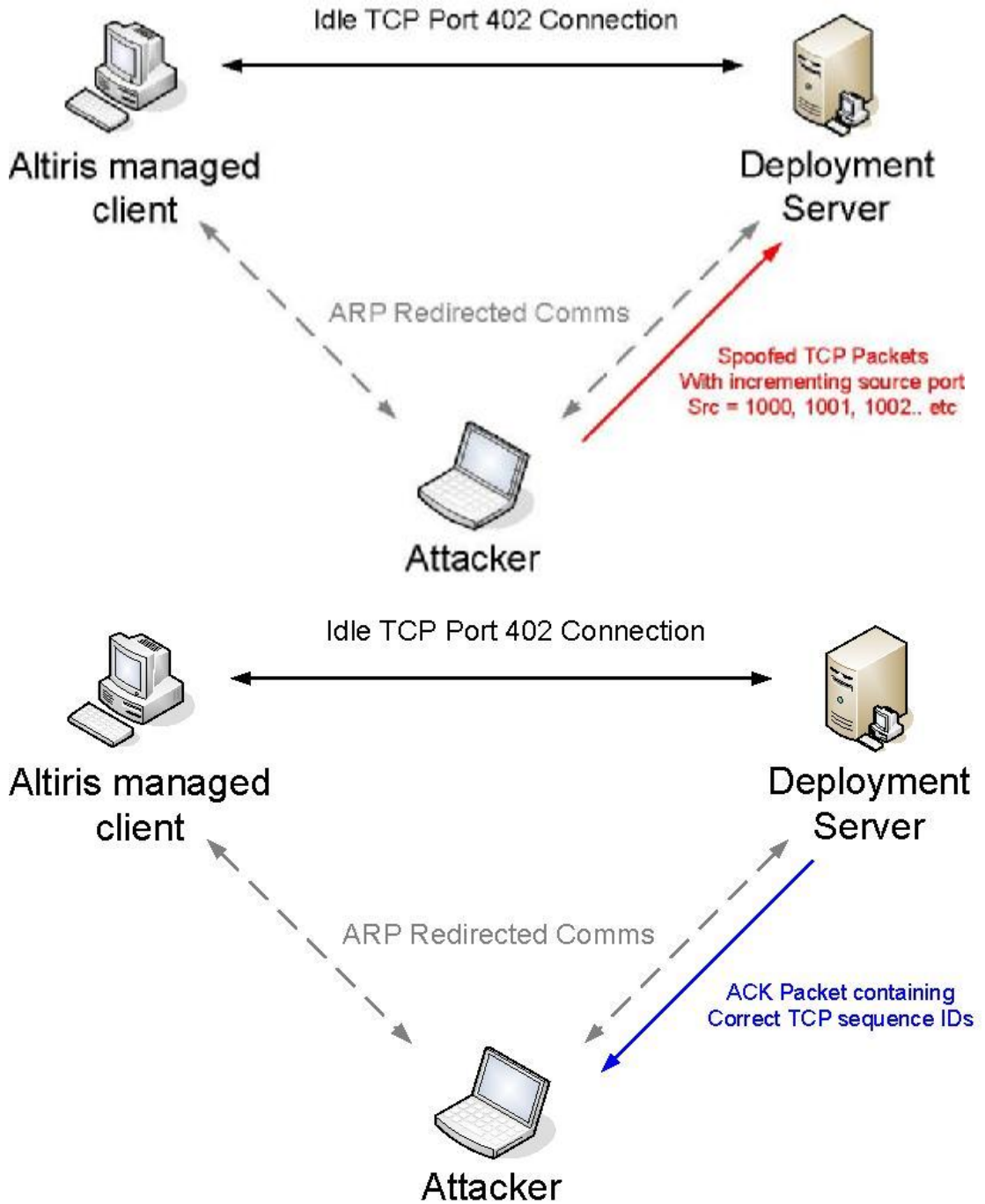
This vulnerability could lead to mobile devices being compromised by external attackers when they are connected to hostile networks, such as public wifi hotspots. This is because as soon as a network connection is made the software agent installed on a client will attempt to communicate with the deployment server. Techniques such as ARP spoofing can be used to intercept these communications and exploit the issue. The risk is exacerbated by the fact that Altiris Deployment Solution supports the use of multicast for locating deployment solutions, which could enable an attacker to exploit this issue without performing traffic redirection attacks, they could even be located on a different network segment to the client machine.

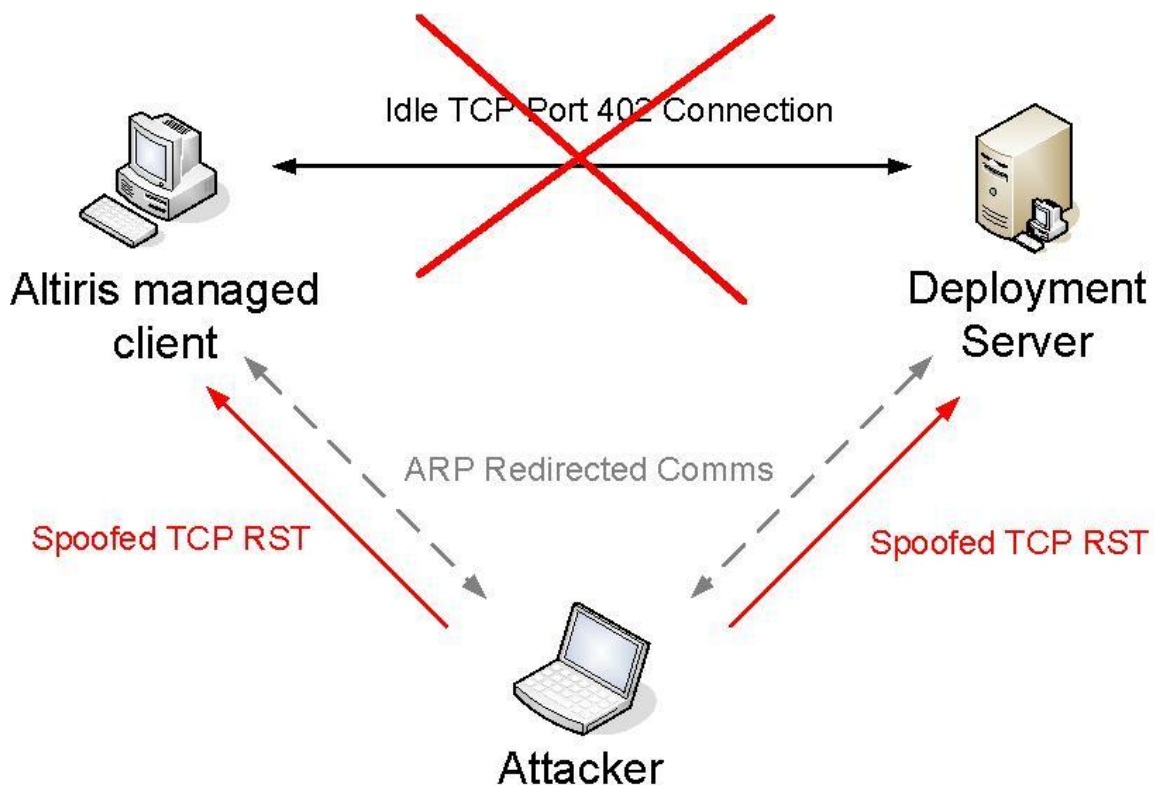
1.5.2 Internal Attacks – Intercepting Internal Communications

If an attacker controls a device on an internal network on which Altiris Deployment Solution is being utilised and they can intercept the communications between a client and the server then they could exploit this issue. However, problems could be introduced by the fact that the TCP connection will probably already be established, authenticated and encrypted, meaning injection of commands into the stream would not be possible. In this case, a reconnect would be required.

In 2004 it was noted in [2] that Altiris did not provide server authentication and these types of attacks were outlined at that time. The author also noted that it would be necessary to wait for a reboot in order to exploit this issue against a client which was already connected using an encrypted connection. However, due to the fact that the client auto-reconnects when the connection has been terminated it is possible to exploit this issue by forcefully terminating the connection. This is trivial using tools such as ettercap [3] and tcpkill [4]; however, this would also require active communication in order to learn the TCP sequence numbers associated with the connection. Communication between the client and server in this case is very infrequent.

A Scapy extension was developed and tested by MWR InfoSecurity which forced communication by brute forcing the TCP source port associated with the connection. This results in an ACK packet being returned by the server which can then be used to learn the sequence numbers and forcefully terminate the connection. The following diagrams demonstrate this process.





When the connection is re-established the traffic interception technique used to force the reconnection can then be used to exploit the client before authentication or encryption has occurred.

1.6 Dependencies

An attacker would need to intercept the communications on TCP port 402 for a client in order to exploit these issues.

2 Recommendations

It is recommended that users should upgrade to the latest Service Pack [5] and ensure that the new software agent is installed on all clients. For a higher level of security assurance, utilise a well scrutinised secure tunnelling mechanism, such as IPSec, SSH or SSL to tunnel the data between clients and the deployment server.

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

4 References

[1] Metasploit

<http://www.metasploit.com/>

[2] Critical Vulnerability in Altiris Deployment Server architecture, Brian Gallagher

<http://archives.neohapsis.com/archives/bugtraq/2004-10/0211.html>

[3] Ettercap

<http://ettercap.sourceforge.net/>

[4] DSniff - tcpkill

<http://monkey.org/~dugsong/dsniff/>

[5] Altiris Patch Information

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