

MWR InfoSecurity Security
Advisory

Symantec's Altiris
Deployment Solution –
DBManager 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.....	4
1.4	Exploit Information	4
1.5	Dependencies	5
2	Recommendations.....	6
3	Further Information	6
4	References.....	7

Affected Software Vulnerability Type

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

CVE Reference	CVE-2009-3107
Author	L. Jennings
Severity	High
Local/Remote	Remote
Vulnerability Class	Logic Flaw
Impact	This issue could potentially be used to gain administrative control over the deployment server and so consequently gain full control over all clients managed by the Altiris Deployment Solution.
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 DBManager service on the deployment server which could allow the service to accept commands without the client providing valid authentication details.

Impact:

This issue could be exploited to allow the unauthenticated remote execution of commands supported by the DBManager service, including the ability to add new users, schedule new tasks and change privilege levels. In addition, MWR InfoSecurity have identified methods of using this access to gain full control of the deployment server.

Control of the deployment server could be used to gain administrative access over all managed clients.

Cause:

The service does not check the client's authentication state when receiving commands; consequently, a malicious client could issue commands directly, without authenticating.

Interim Workaround:

Block access to the DBManager service (TCP port 505 by default) using network or host based filtering controls.

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

One of the services that is installed on the deployment server is the DBManager service, which is intended to act as a interface between the Altiris console and the database and the console and the server[1]: -

“This component is used for secure communication between the Console and the Database and the Console and the Server.”

This service listens by default on TCP port 505. A proprietary ASCII based protocol is then used to facilitate communication. This is encrypted by default during the handshake. It was possible to analyse the binary by disassembly and debugging techniques and so determine the format of the protocol and the commands available. Examples of a limited number of the commands that are available are listed below: -

- ScheduleEvent
- AddUser
- SetPrivilege
- UpdatePXEBootOptions

1.3 Vulnerability Details

The code implementing the protocol handling does not properly track the state of authentication. 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 client which does not use the protocol in the intended manner to issue commands to the DBManager service without authentication. This can be achieved by issuing commands without first making an authentication request.

1.4 Exploit Information

MWR InfoSecurity have discovered a number of methods which can be used to access the functionality that is available to gain full, general administrative control over the deployment server by controlling the database content. This level of access

could also be used to gain full control over all the clients that are managed using Altiris.

1.5 Dependencies

An attacker would need to be able to contact the DBManager service on the deployment server (default TCP port 505). This service listens externally by default. Database privileges would affect the ability of an attacker to extend their access to more general control of the database server.

2 Recommendations

It is recommended that users should upgrade to the latest service pack [2] and ensure that the new software agent is installed on all clients. For a higher level of security assurance, it is recommended that access to TCP port 505 is also prevented using network filtering controls to ensure that only those management clients who require access to this port are able to do so. In many environments this could be restricted to localhost only.

Standard database lockdown procedures could also help to prevent this vulnerability being used to gain operating system level control of the database server. These procedures should include the use of a low privileged service account and limiting the ability to execute operating system commands and to access the underlying file system.

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] Altiris Deployment Solution Admin Guide
http://www.altiris.com/upload/deployment_004.pdf

[2] 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