

MWR InfoSecurity Security
Advisory

Symantec's Altiris
Deployment Solution – File
Transfer Race Condition

7th January 2010



Contents

1	Detailed Vulnerability Description	4
1.1	Introduction	4
1.2	Technical Background.....	4
1.3	Vulnerability Details.....	5
1.4	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:	Versions prior to 6.9 SP3

CVE Reference	CVE-2009-3110
Author	L. Jennings
Severity	Medium
Local/Remote	Remote
Vulnerability Class	Race Condition
Impact	An attacker could gain access to the contents of files transferred to clients and prevent clients from receiving them.
Vendor Response	The vendor has addressed the issue in a new Service Pack
Exploit Details Included	Yes
Affected OS	Microsoft Windows

Overview:

A race condition vulnerability has been identified in the service that enables file transfer functionality between the deployment server and its clients.

Impact:

A remote attacker who was able to communicate with the deployment server could intercept the contents of files destined for clients and prevent their delivery. This would enable sensitive information within these files to be compromised and a denial of service of file transfer functionality to be achieved.

Cause:

An out of band network service is used for the transfer of file contents after a file transfer request has been agreed using the control channel between client and server. This out of band service provides no authentication or session control and so the first user to make a request receives the file contents.

Interim Workaround:

Enabling encrypted communications between the clients and deployment server would prevent disclosure of the file contents but would not prevent a denial of service condition being achievable. Limiting network access to the file transfer service to the relevant clients' IP addresses would reduce this risk.

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

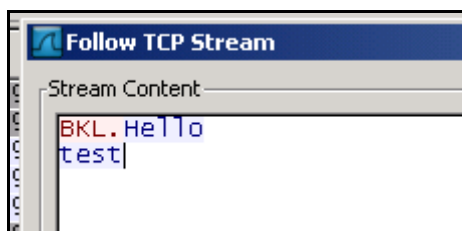
"Altiris Deployment Solution 6.9 software helps reduce the cost of deploying and managing servers, desktops, notebooks, and thin clients from a centralized location in your environment. An easy-to-use, automated deployment solution offers OS deployment, configuration, PC "personality" migration, and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

1.2 Technical Background

The Altiris Deployment Solution provides the ability to transfer files to its clients. The file transfer requests are made by the server using the control channel operating by default on TCP port 402. An example of this communication can be seen in the packet dump given below: -

```
.Request=SendFile
Filename="c:\test2dlha.txt"
Date=1257710486
Attributes=32
Size=11
Port=1051
Schedule-ID=100000019
Task-Sequence-ID=0
Task-Type=CopyFile
Allow-Defer=5
CurrentFileCount=1
TotalFileCount=1
TotalFileCopySize=11
ID=5000002
.Reply=SendFile
Schedule-ID=100000019
Task-Sequence-ID=0
Result=Success
Status-Code=0
Status-Module=AClient
```

As can be seen, the transfer request also includes a port number. This represents an out of band communication channel for the transfer of the file's contents. The client will then connect to this TCP port and send a 'magic packet' in order to receive the contents of the file from the deployment server. An example of this communication can be seen in the following packet dump: -



```
Follow TCP Stream
Stream Content
BKL.Hello
test|
```

1.3 Vulnerability Details

The magic packet that is sent is all that is required in order to receive the file data. There is no identifier requested or session state tracked and so the file contents will be delivered on a first-come first first-serve basis. It is therefore trivial to write a multi-threaded client which continually makes requests to this service in order to retrieve the contents of any file that is transferred from the deployment server to any client whilst simultaneously preventing the delivery of any files to any clients.

1.4 Dependencies

An attacker would require network connectivity to the deployment server on the port used for the file transfer service. This port is dynamic and appears to be assigned randomly at the installation stage.

2 Recommendations

It is recommended that users upgrade to the latest Service Pack [1] and ensure that the new software agent is installed on all clients. As an alternative or additional security control, access to the file transfer port should be restricted to the IP addresses of valid clients only, and encryption should be enabled to prevent the disclosure of the file contents to an attacker.

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 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