

Cisco Security Agent

0-Day Protection against the WMF Exploit



CSA Protection - WMF Exploit

CSA Provides 0-Day Protection Against WMF Exploit

PRIVEON

- 0-Day Exploit

- Bugtraq Post on 12/27

“Warning the following URL successfully exploited a fully patched windows xp system with a freshly updated norton anti virus.

unionseek.com/d/t1/wmf_exp.htm

The url runs a .wmf and executes the virus”

- SANS – Internet Storm Center 12/28

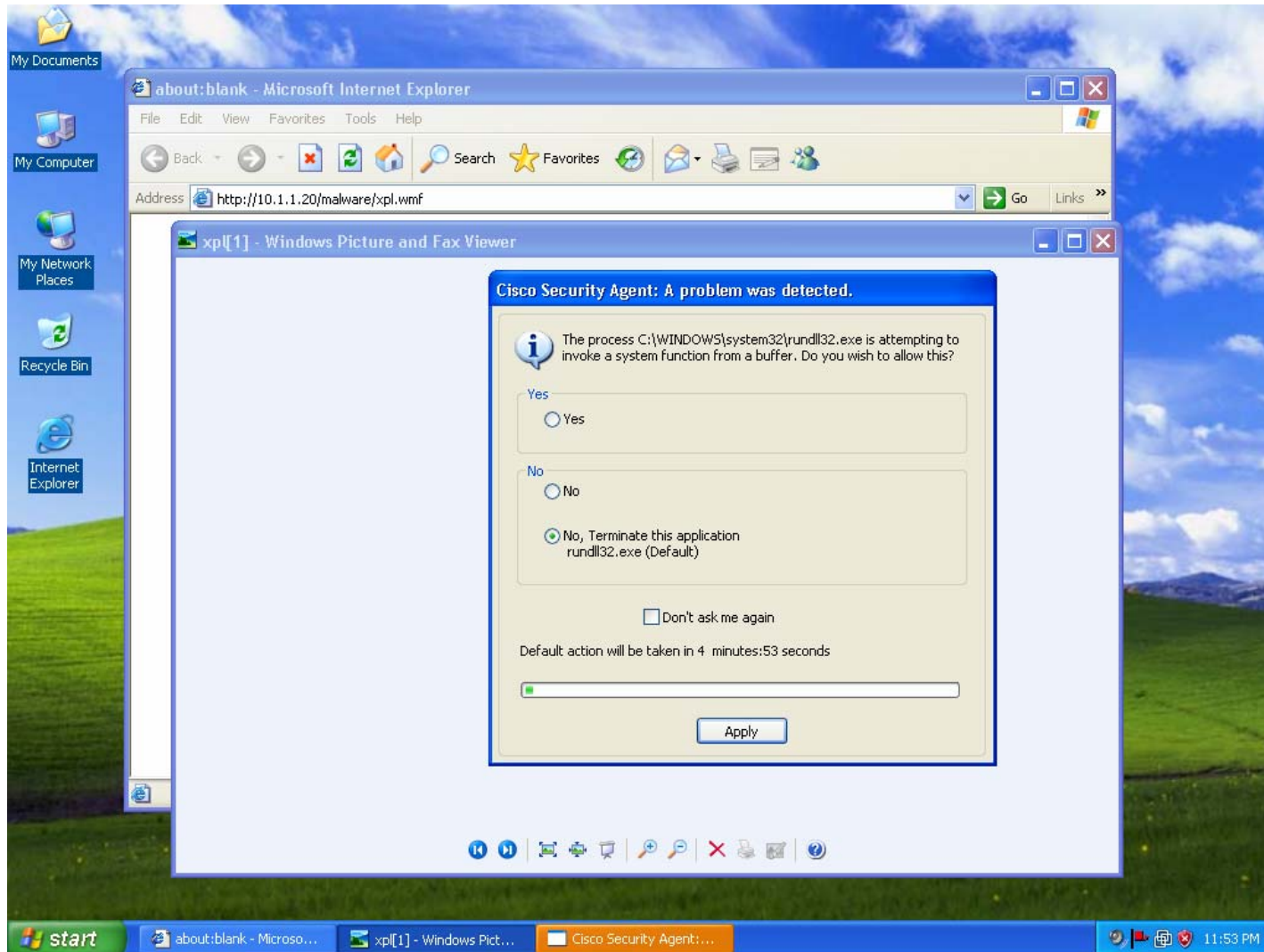
“We are moving to Infocon Yellow for a bit. There has been some debate among the handlers about this step, but considering that a lot of people are on holidays and might otherwise miss the WMF 0-day problem, we have decided to raise the alert level.”

“While the original exploit only referred to the Microsoft Picture and Fax Viewer, current information is that any application which automatically displays or renders WMF files is vulnerable to the problem. This includes Google Desktop, if the indexing function finds one of the exploit WMFs on the local hard drive ...”

CSA Protection - WMF Exploit

CSA Stops Code Execution from Buffer Overflow

PRIVEON



CSA Protection - WMF Exploit

CSAMC Event Details

The screenshot displays the Management Center for Cisco Security Agents V4.5 interface. The main window shows the details of a security event. On the left, a sidebar lists 'Events > Event Log' with a table of recent events. The main content area is titled 'Policy rule details' and 'Event details'.

#	Date	Host
266	12/29/2005 12:53:38 AM	XPSP2
265	12/29/2005 12:53:37 AM	XPSP2
264	12/29/2005 12:47:53 AM	XPSP2

Policy rule details:

Description	Network Applications, Access system functions from a buffer
Module	General Application Permissions - all Security Levels [W, V4.5.1 r639]
Cisco Security Agent query	<p><i>English:</i> The process @appname is attempting to invoke a system function from a buffer. Do you wish to allow this?</p> <p><i>Spanish:</i> El proceso @appname intenta invocar una función del sistema desde un búfer. ¿Desea permitirlo?</p> <p><i>French:</i> Le processus @appname tente d'invoquer la fonction système à partir d'un tampon. Voulez-vous autoriser cette opération ?</p> <p><i>German:</i> Der Prozess @appname versucht, eine Systemfunktion, aus einem Puffer aufzurufen. Soll dieser Vorgang zugelassen werden?</p> <p><i>Italian:</i> Il processo @appname sta tentando di richiamare una funzione di sistema da un buffer. Autorizzare questa operazione?</p> <p><i>Japanese:</i> @appname @@@@@@ @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@</p> <p><i>Korean:</i> @appname@() @@@@ @@@ @@@ @@@ @@@ @@@ @@@@@@?</p> <p><i>Simplified Chinese:</i> @appname @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@</p>

Event details:

Event Text	The process 'C:\WINDOWS\system32\rundll32.exe' (as user XPSP2\Joe User) attempted to call the function CreateFileA("a.exe") from a buffer (the return address was 0xc60e4). The code at this address is '32c05050 b040c1e0 1850ff75 38ff5508 89454433 c066b80c 012be08b f48d5e04'. This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. The user was queried and a 'Terminate' response was received.
Event Time	server: 12/29/2005 12:53:37 AM; agent: -1 hour
Code	HACL_OVERFLOW_QUERY
Plnt	4
Plnt2	172
PString	C:\WINDOWS\system32\rundll32.exe
time	329.8 (seconds since boot)
type	APICALL
ProcessId	1216
ApiOperation	BufferOverflowDetected
Credentials	os=win32,T=XPSP2\Joe User,t=0105000000000005150000078006D1FA020966A07E53B2BE8030000,G=XPSP2\None,g=0105000000000005150000078006D1FA020966A07E53B2B01020000
ApiPlnt1	811236
ApiPString1	32c05050 b040c1e0 1850ff75 38ff5508 89454433 c066b80c 012be08b f48d5e04

CSA Protection - WMF Exploit

CSAMC Event Details (cont...)

The screenshot displays the Cisco Management Center for Security Agents V4.5 interface. The main window shows the details of an event with the following information:

- ApiOperation:** BufferOverflowDetected
- Credentials:** os=win32,T=XPSP2\Joe
User,t=01050000000000051500000078006D1FA020966A07E53B2BEB030000,G=XPSP2
\None,g=0105000000000005 150000078006D1FA020966A07E53B2B01020000
- ApiPInt1:** 811236
- ApiPString1:** 32c05050 b040c1e0 1850ff75 38ff5508
89454433 c066b80c 012be08b f48d5e04
- ApiPString2:** CreateFileA
- ApiPInt2:** 12188364
- ApiPString3:** 00fbbb900 e4600c00 f0fab900 00000040
00000000 00000000 02000000 82000000
00000000 612e6578 65000000 7769e669
6e657400 00000000 771d807c 241a807c
- args(4):** a.exe
- ApiPInt3:** 811220
- argi(4):** 1
- FlattenedForm:** (t-1135835616 n-695625000 z--21600 sm-114 sc-13 dm-1 dc-7 cd-555 hp-2 p*(i-4 i-172 w-
C:\WINDOWS\system32\rundll32.exe r*(type-17 time-3298 pnd-83888257 rapi*(pid-1216 op-8 p*(i-811236 d-
Yamuqlqbdogg9FD48FvIkYrendWMHldbSc4IsJJEra a-CreateFileA i-12188364 d-
aSFUaqoymaa86NlaaaaaabaaaaaaaaaacaaiiaaaaaaaaaaH5sz4vgaaaWDP5wAUvgDaaaaaWDDaiFKObG8b
a-a.exe i-811220 i-1) cr-Owin32%00TSPSP2\Joe%20User%
00t01050000000000051500000078006D1FA020966A07E53B2BEB030000%00GXSPSP2\ None%
00g0105000000000005150000078006D1FA020966A07E53B2B01020000%00)))
- Disassembly:**

Address	Code	Instruction
000c60d4	32c0	xor al,al
000c60d6	50	push eax
000c60d7	50	push eax
000c60d8	b040	mov al,0x40
000c60da	c1e018	shl eax,0x18
000c60dd	50	push eax
000c60de	ff7538	push dword[ss:ebp+0x38]
000c60e1	ff5508	call dword[ss:ebp+0x8]
000c60e4**	894544	mov dword[ss:ebp+0x44],eax
000c60e7	33c0	xor eax,eax
000c60e9	66b80c01	mov ax,0x10c
000c60ed	2be0	sub esp,eax
000c60ef	8bf4	mov esi,esp
000c60f1	8d5e04	lea ebx,[esi+0x4]

CSA Protection - WMF Exploit

CSAMC Default Desktop Policies (CSA 4.5.1.639)

The screenshot shows the Management Center for Cisco Security Agents V4.5 web interface. The browser address bar shows the URL: https://dell750-2/csamc45/webadmin. The interface includes a navigation menu with options like Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The main content area is divided into two sections: Attached Policies and Combined Policy Rules.

Attached Policies

Policy Name	Version	Description	Rule Modules
Document Security - Windows	4.5.1 r639	Policy to protect user documents	1 module
Email Client - Basic Security - Windows	4.5.1 r639	Basic application enforcement policy for email client software.	3 modules
General application - Basic Security - Windows	4.5.1 r639	Basic, Application independent security policy for Windows	3 modules
Installation Applications - Windows	4.5.1 r639	Software Installers for Windows	4 modules
IP Stack - Internal Network Security	4.5.1 r639	Policy for protecting the IP Stack on internal systems	1 module
Network Personal Firewall	4.5.1 r639	Control network access and provide some end user access controls.	1 module
Operating System - Base Protection - Windows	4.5.1 r639	Basic protection for Windows OS	5 modules
Virus Scanner - Windows	4.5.1 r639	Application enforcement policy for virus scanner software.	1 module

Combined Policy Rules

View **All** rules

Enforce rules: 121 (click the header links to sort)

ID	Type	Status	Action	Log	Description	Rule Module
529	Application control	Enabled	⊘	⊘	Email applications, invoke Cmd Shells...	Email Client Module - base security [V4.5.1 r639]
526	File access control	Enabled	⊘	⊘	Email applications, read/write dynamically quarantined files	Email Client Module - base security [V4.5.1 r639]
64	Network access control	Disabled	⊘	⊘	All Applications, server for TCP and UDP services	Installation - Application Permissions Module [V4.5.1 r639]
113	Registry access control	Enabled	⊘	⊘	Applications processing untrusted content, write Local User Account keys	System Hardening Module [V4.5.1 r639]
600	Application control	Enabled	✔	⊘	All Applications, Invoke MS sysocmgr	Installation - Application Detection - Install detected [V4.5.1 r639]
160	Application control	Enabled	✔	⊘	All Applications, Installing MS sysocmgr	Installation - Application Detection - Install detected [V4.5.1 r639]

Buttons: Save, Delete, Reset Cisco Security Agents, No rule changes pending, Generate rules. Logged in as: lboggis

CSA Protection - WMF Exploit

CSAMC Event Details (cont...)

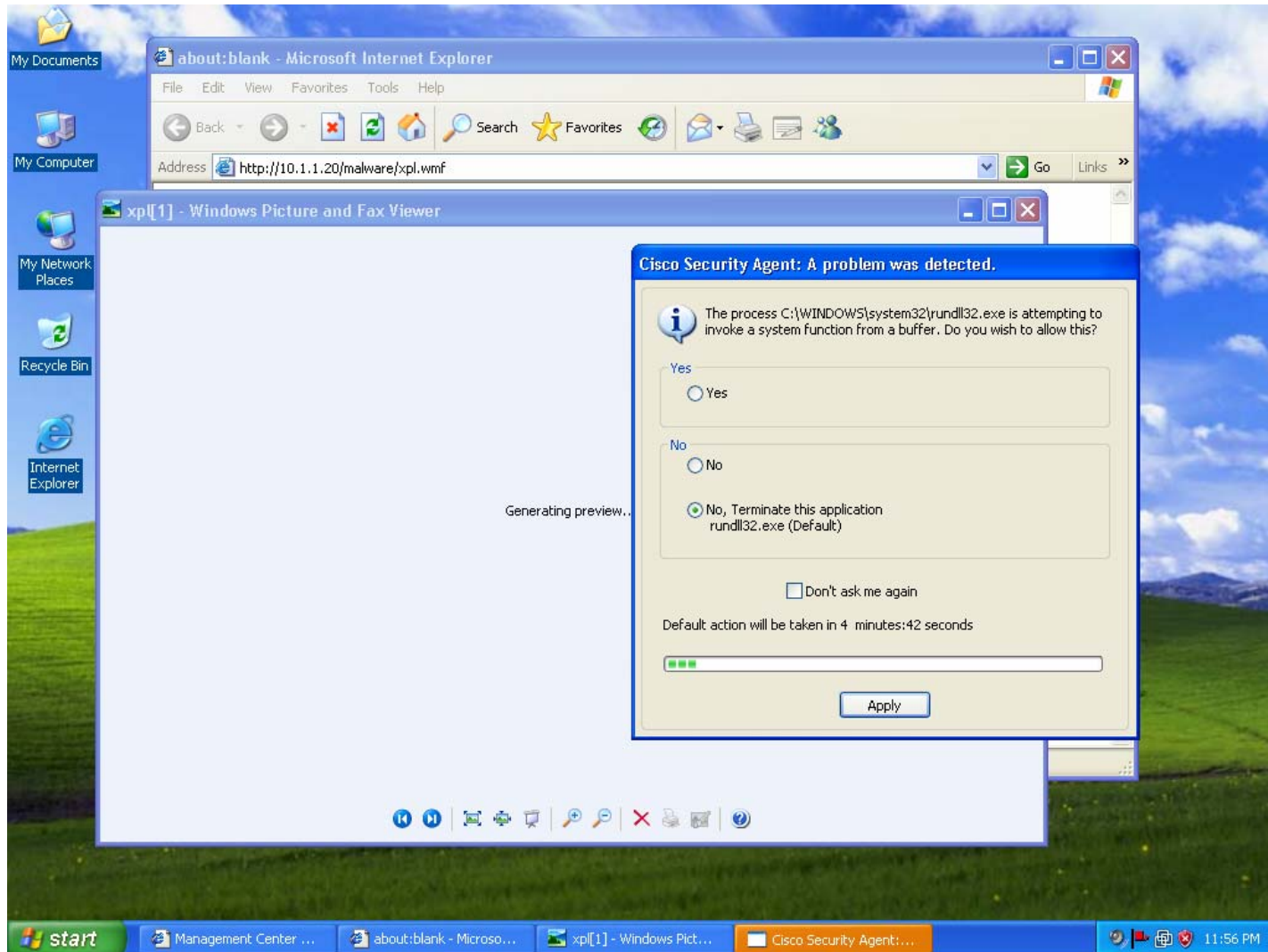
- The following slides step the user through the entire WMF exploit and a Spyware version of payload execution to demonstrate how CSA provides protection at all levels using default desktop policies.

Note: This is for demonstration purposes only. In a normal CSA deployment the user would not see any of these query messages. CSA would provide protection without user interaction.

CSA Protection - WMF Exploit

Step 1: Buffer Overflow and Code Execution

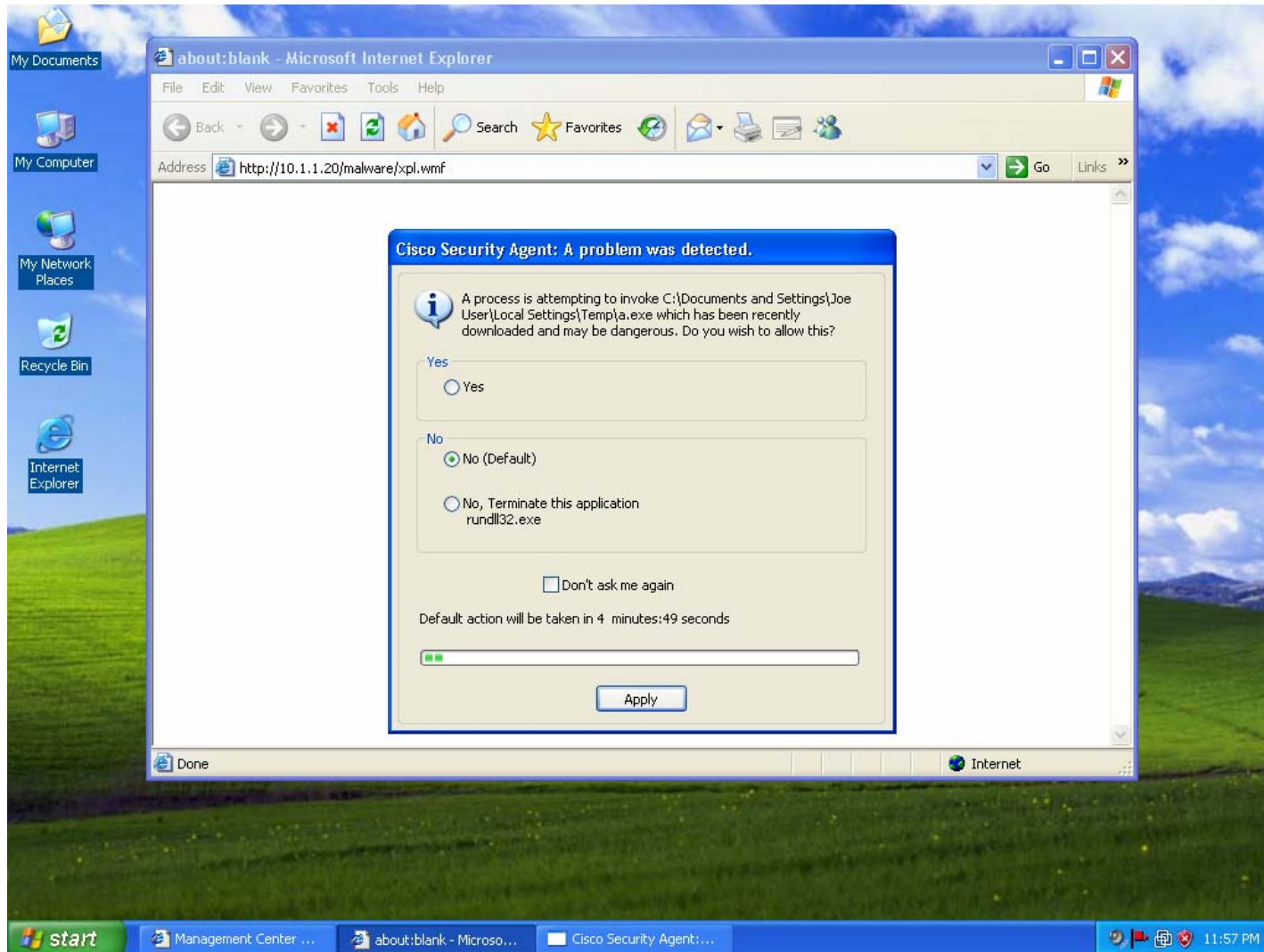
PRIVEON



CSA Protection - WMF Exploit

Step 2: Tries to Run Payload (a.exe)

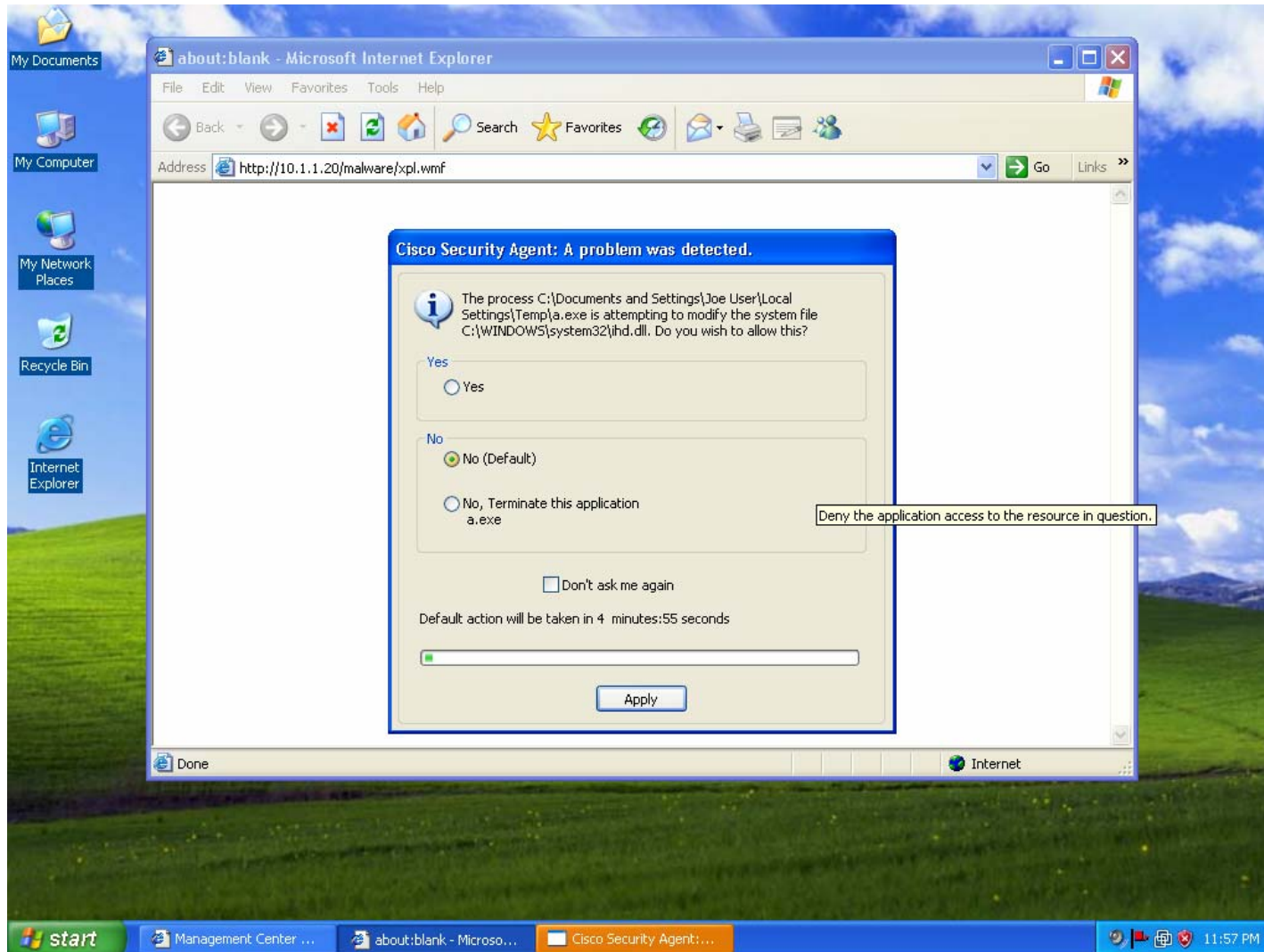
PRIVEON



CSA Protection - WMF Exploit

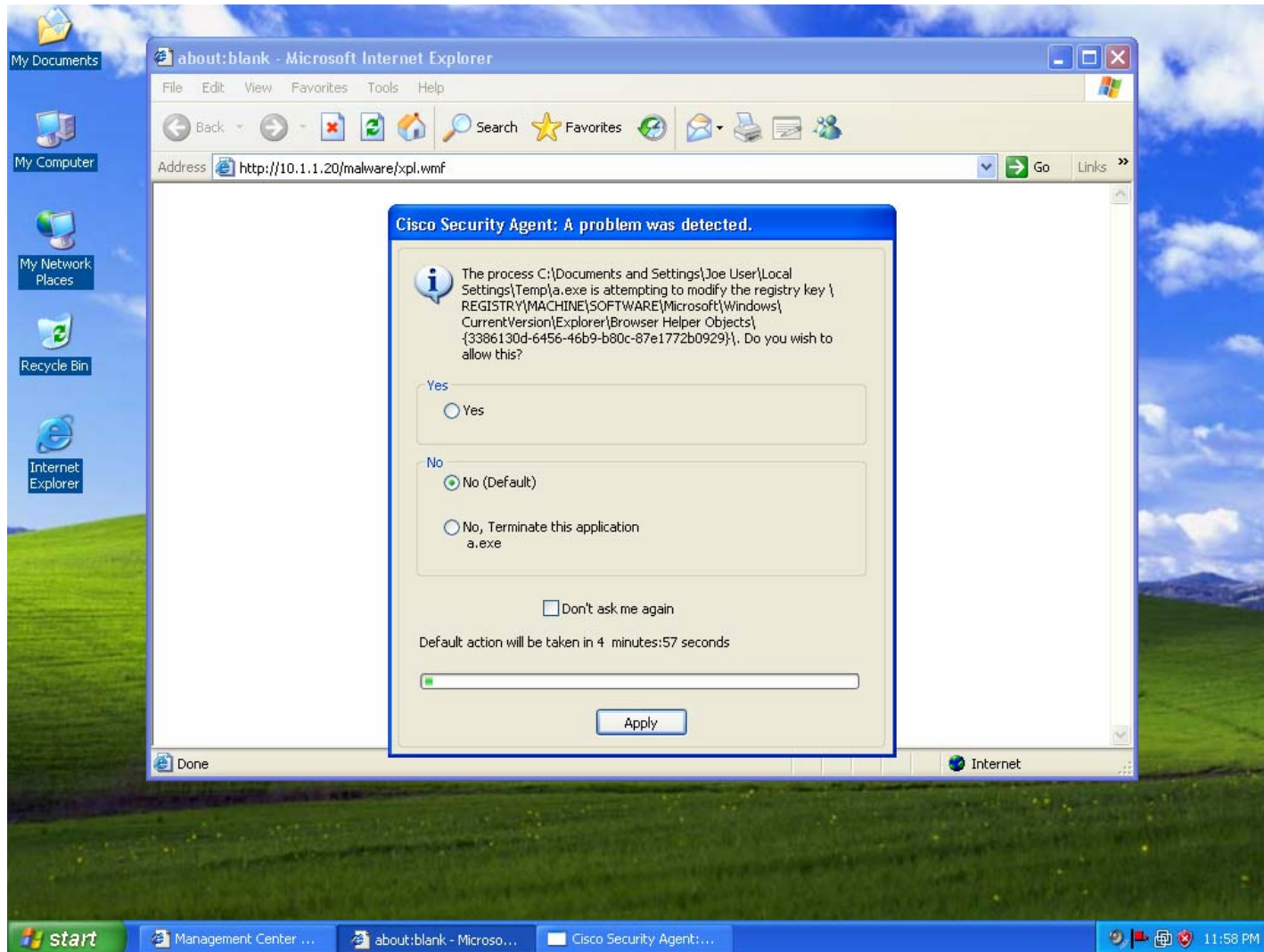
Step 3: Payload Tries to Write DLL to System Folder

PRIVEON



CSA Protection - WMF Exploit

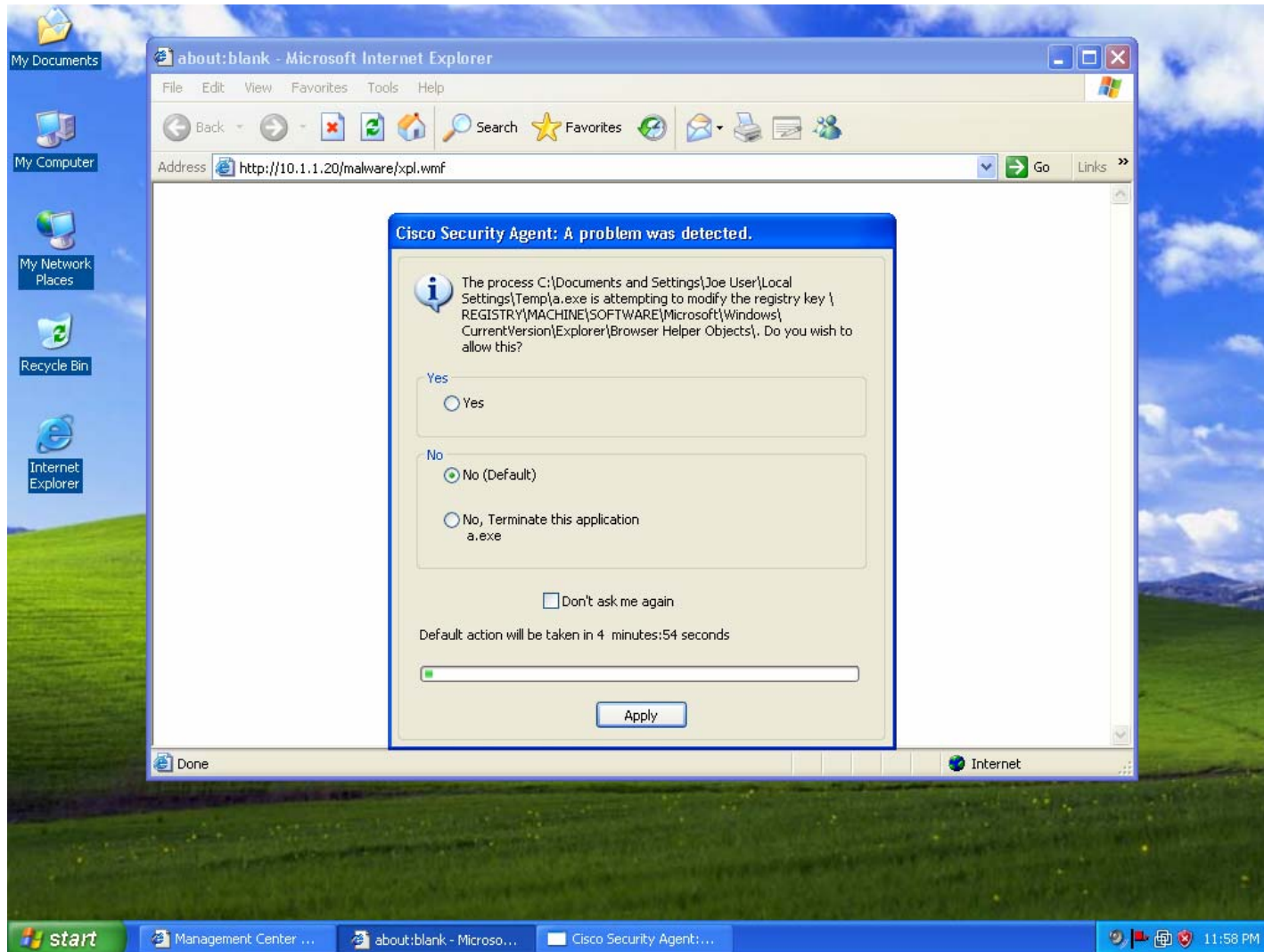
Step 4: Payload Tries to Modify Registry



CSA Protection - WMF Exploit

Step 5: Payload Tries to Modify Registry (cont...)

PRIVEON



CSA Protection - WMF Exploit

CSAMC Event Details (Steps 1-5)

The screenshot displays the Management Center for Cisco Security Agents V4.5 web interface. The browser address bar shows `https://dell750-2/csamc45/webadmin`. The interface includes a navigation menu with options like Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. A table of security events is shown, with the following details:

#	Date	Host	Severity	Event
271	12/29/2005 12:59:18 AM	XPSP2	Notice	The process 'C:\Documents and Settings\Joe User\Local Settings\Temp\a.exe' (as user XPSP2\Joe User) attempted to access the registry key '\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects', value ". The attempted access was a write (operation = CREATE/KEY). The user was queried and a 'Yes' response was received. Details Rule 131 Wizard Find Similar
270	12/29/2005 12:58:49 AM	XPSP2	Notice	The process 'C:\Documents and Settings\Joe User\Local Settings\Temp\a.exe' (as user XPSP2\Joe User) attempted to access the registry key '\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{3386130d-6456-46b9-b80c-87e1772b0929}', value ". The attempted access was a write (operation = CREATE/KEY). The user was queried and a 'Yes' response was received. Details Rule 131 Wizard Find Similar
269	12/29/2005 12:58:20 AM	XPSP2	Notice	The process 'C:\Documents and Settings\Joe User\Local Settings\Temp\a.exe' (as user XPSP2\Joe User) attempted to access 'C:\WINDOWS\system32\ihd.dll'. The attempted access was a write (operation = OPEN/CREATE). The user was queried and a 'Yes' response was received. Details Rule 130 Wizard Find Similar
268	12/29/2005 12:57:43 AM	XPSP2	Notice	The current application 'C:\WINDOWS\system32\rundll32.exe' (as user XPSP2\Joe User) tried to execute the new application 'C:\Documents and Settings\Joe User\Local Settings\Temp\a.exe'. The user was queried and a 'Yes' response was received. Details Rule 511 Wizard Find Similar
267	12/29/2005 12:57:06 AM	XPSP2	Notice	The process 'C:\WINDOWS\system32\rundll32.exe' (as user XPSP2\Joe User) attempted to call the function CreateFileA("a.exe") from a buffer (the return address was 0xc5d6c). The code at this address is '32c05050 b040c1e0 1850ff75 38ff5508 89454433 c066b80c 012be08b f48d5e04'. This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. The user was queried and a 'Yes' response was received. Details Rule 172 Wizard Find Similar

At the bottom of the interface, there is a status bar indicating "No rule changes pending" and "Generate rules". The user is logged in as "iboggis".

CSA Protection - WMF Exploit

Reference Material

PRIVEON

**For Additional Information see US-CERT
(VU#181038)**

<http://www.kb.cert.org/vuls/id/181038>

- <http://www.us-cert.gov/cas/techalerts/TA05-362A.html>
<http://www.microsoft.com/technet/security/advisory/912840.msp>
<http://isc.sans.org/diary.php?rss&storyid=972>
<http://isc.sans.org/diary.php?storyid=975>
<http://secunia.com/advisories/18255/>
<http://www.securityfocus.com/bid/16074>
http://vil.mcafeesecurity.com/vil/content/v_137760.htm
<http://www.f-secure.com/weblog/archives/archive-122005.html#00000753>
<http://www.symantec.com/avcenter/venc/data/bloodhound.exploit.56.html>
<http://www.ciac.org/ciac/bulletins/q-085.shtml>

<http://www.priveon.com>

