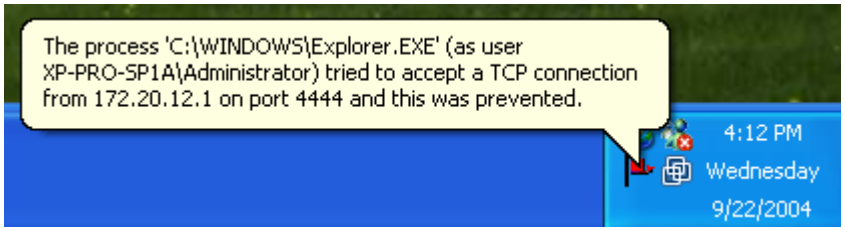
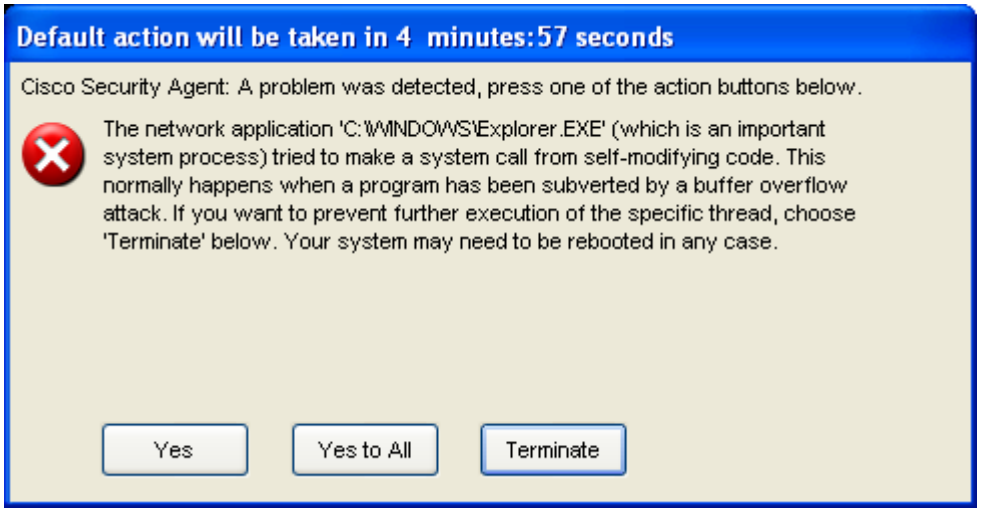
CSA in Action: Protection JPEG (GDI+) OVERFLOW

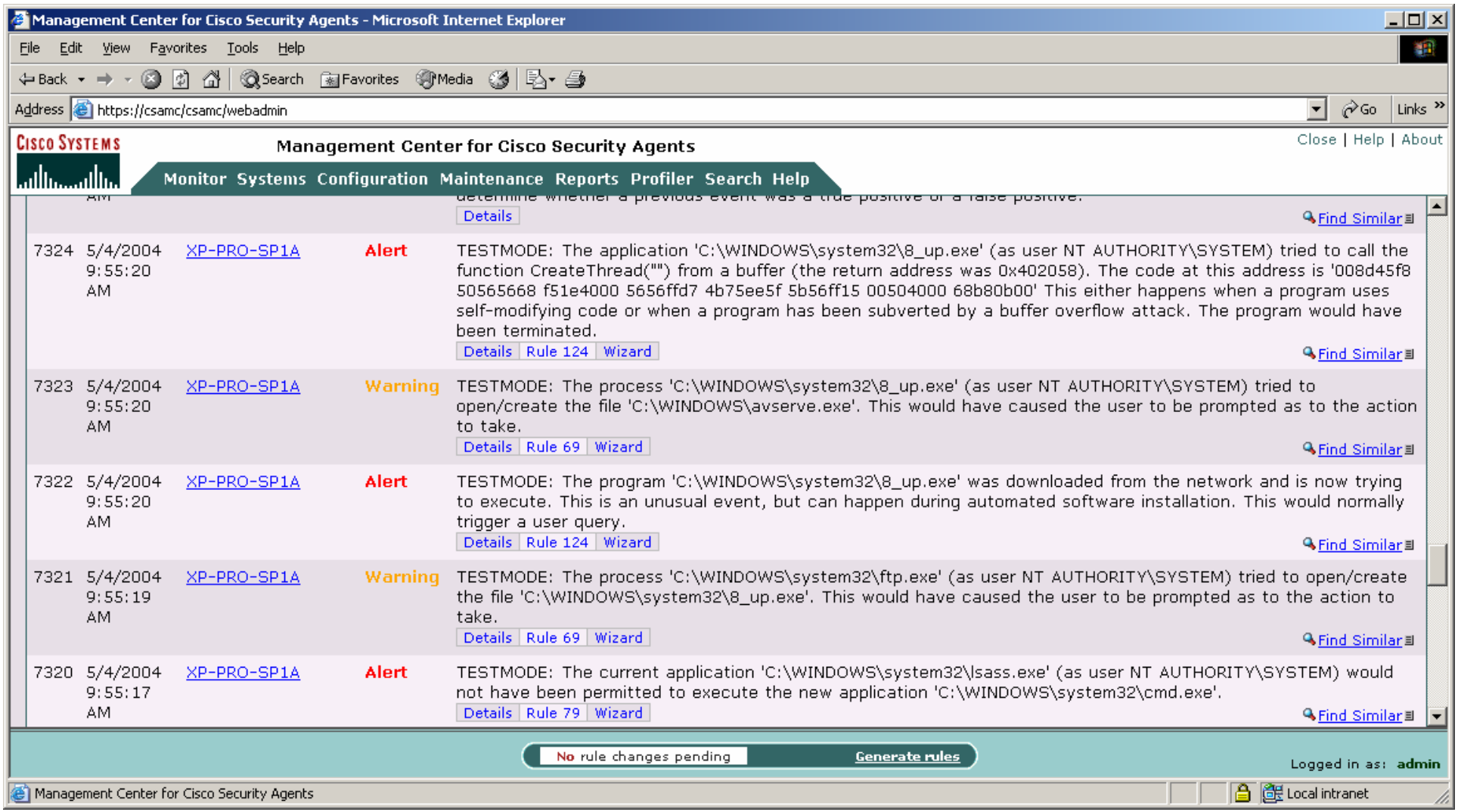
Cisco.com

6	9/22/2004 5:12:48 PM	XP-PRO-SP1A	Alert	The process 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to accept a TCP connection from 172.20.12.1 on port 4444 and this was prevented. Details | Rule 507 | Wizard Find Similar
5	9/22/2004 5:10:03 PM	XP-PRO-SP1A	Warning	The critical system application 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to call the function CreateProcessA("CMD") from a buffer (the return address was 0x19163cb). The code at this address is '515351ff 75006872 feb316ff 5504ffd0 89e6ff75 0068add9 05ceff55 0489c36a' This either happens when a program uses self-modifying code or when a program has been subverted by a buffer overflow attack. The user chose 'Yes'. Details | Rule 97 Find Similar





CSA in Action: Protection Against Sasser



CSA in Action: Protection Against MyDoom

Cisco.com

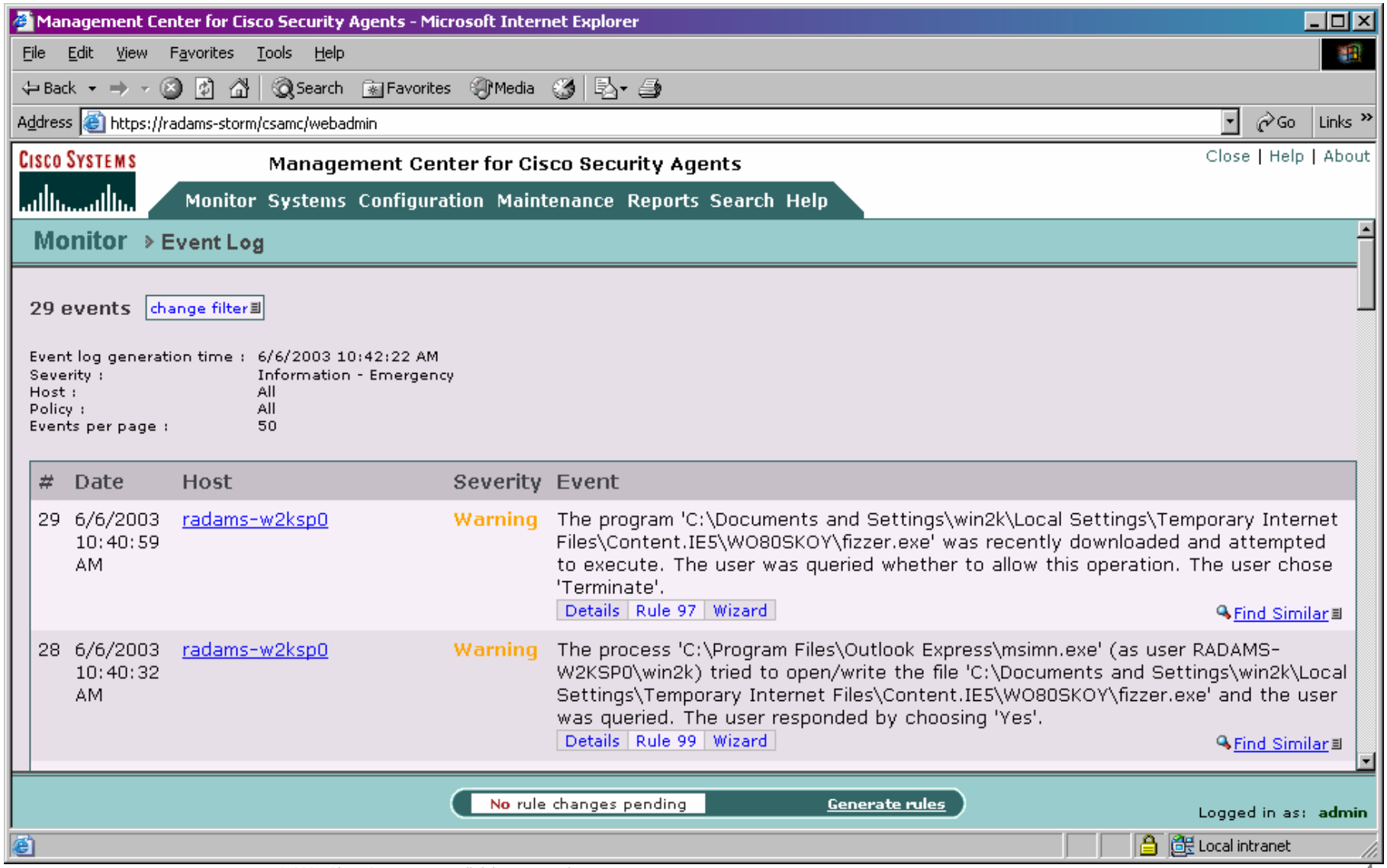
[2004-01-26 23:48:40]: The process 'D:\Documents and Settings\vbieri\Local Settings\Temp\message.scr' (as user EMEA\vbieir) tried to open/create the file 'C:\WINNT\system32\shimgapi.dll' **and the user was queried. The user responded by choosing 'No'.**

[2004-01-26 23:48:44]: Event: The process 'D:\Documents and Settings\vbieri\Local Settings\Temp\Rar$DI00.572\document.scr' (as user EMEA\vbieri) tried to write-value the registry **key'\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\Windows** CURRENTVERSION\Run', value 'TaskMon' **and the user was queried. The user responded by choosing 'No'.**

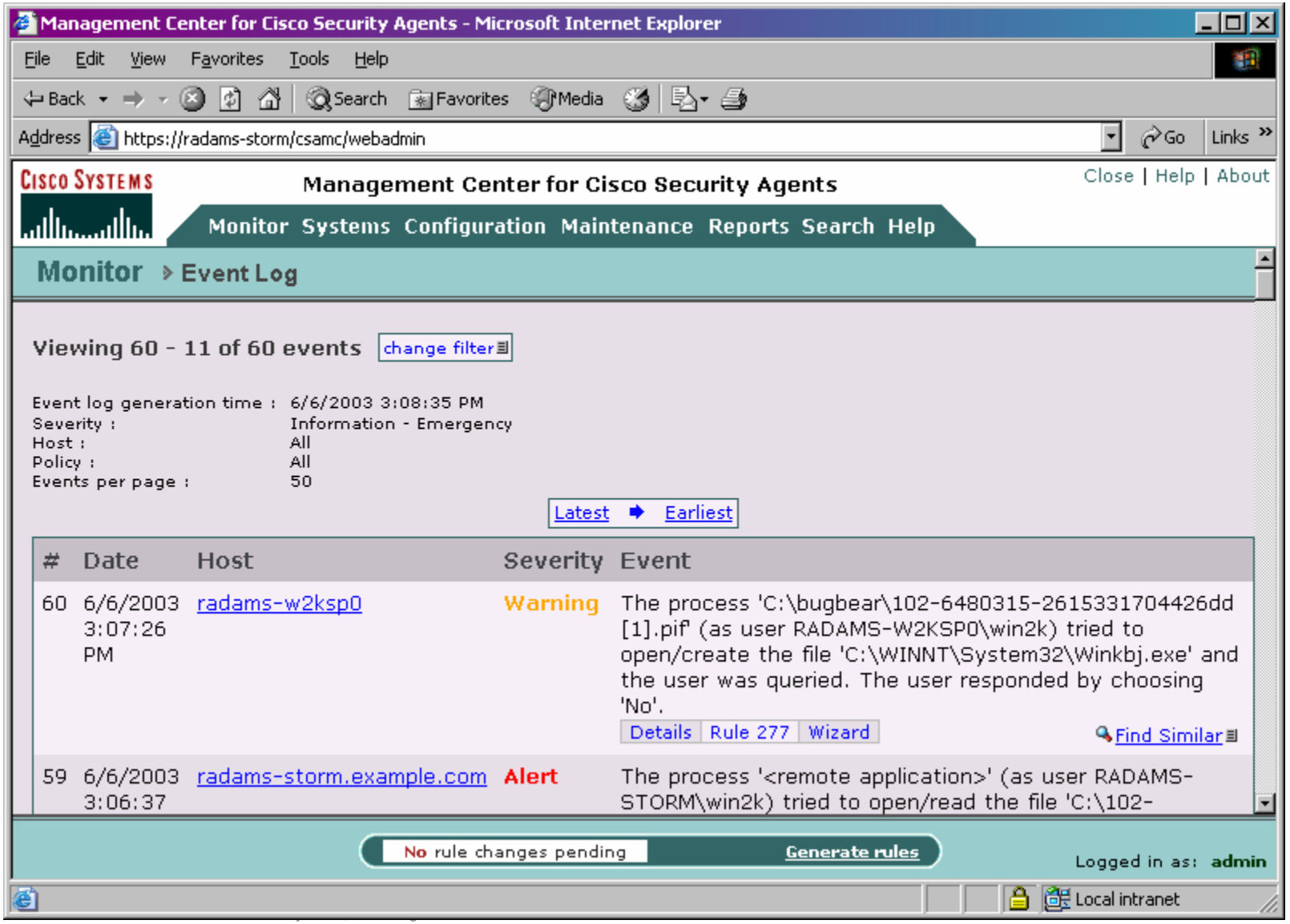
[2004-01-26 23:49:06]: Event: Potential worm propagation**: The process 'D:\Documents and Settings\vbieri\Local Settings\Temp\Rar$DI00.572\document.scr' (as user EMEA\vbieri) has read downloaded content (file D:\Documents and Settings\vbieri\Local Settings\Temp\Rar$DI00.572\document.scr) and** attempted to access an email or network related resource (vbieri.wab).**This is considered suspect. The user chose 'Terminate'.**

[2004-01-26 23:49:23]: The process 'D:\Documents and Settings\vbieri\Local Settings\Temp\message.scr' (as user EMEA\vbieri) tried to write-value the registry key **'\REGISTRY\USER\S-1-5-21-1801674531-2025429265-839522115-189223\SOFTWARE\MICROSOFT\Windows\CURRENTVERSION\Explorer\Shell Folders', value 'History' and the user was queried. The user responded by choosing 'No'.**

CSA in Action: Protection Against Fizzer

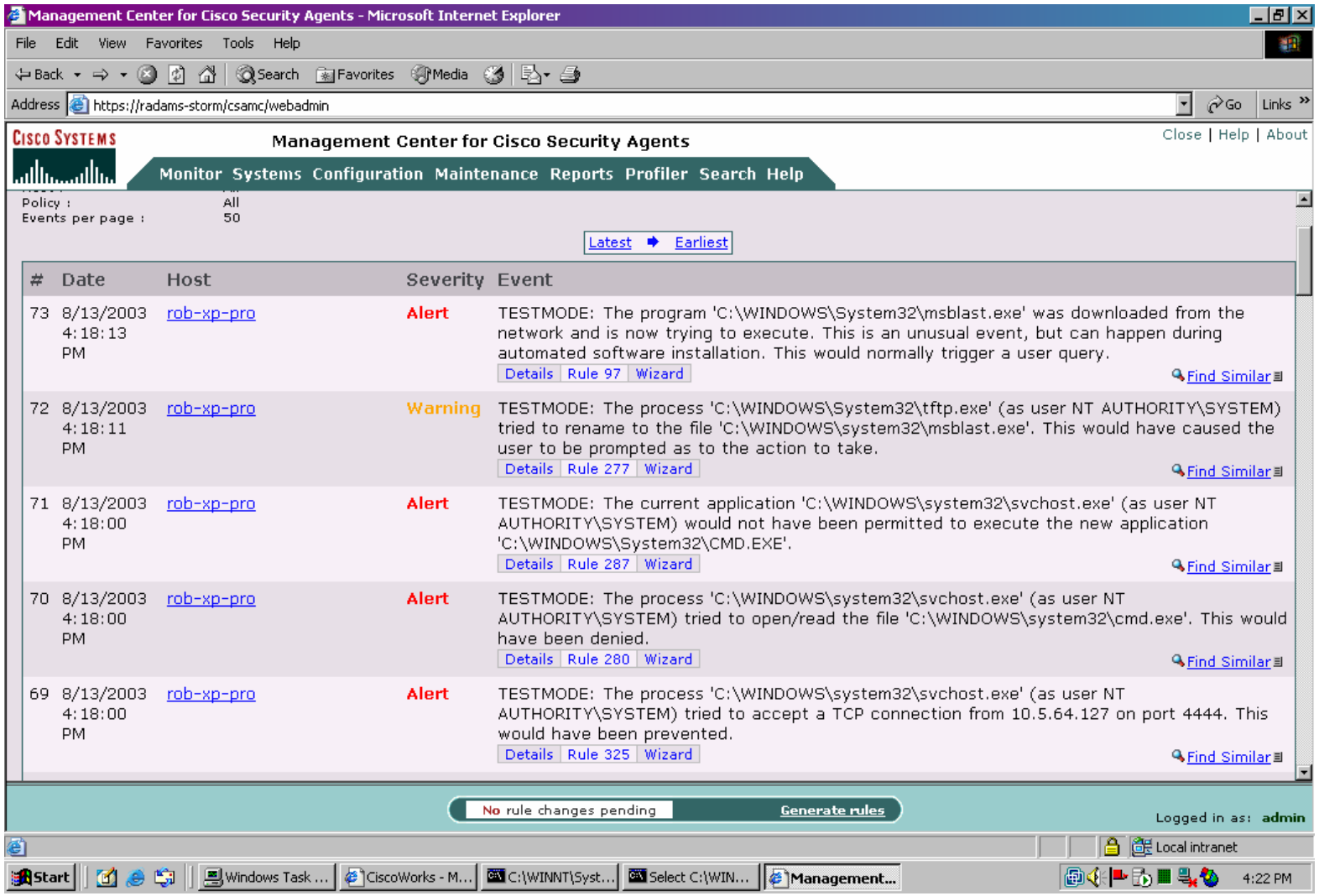


CSA in Action: Protection Against BugBear



CSA in Action: Protection Against Blaster

Cisco.com



CSA in Action: Protection Against Slammer

Cisco.com