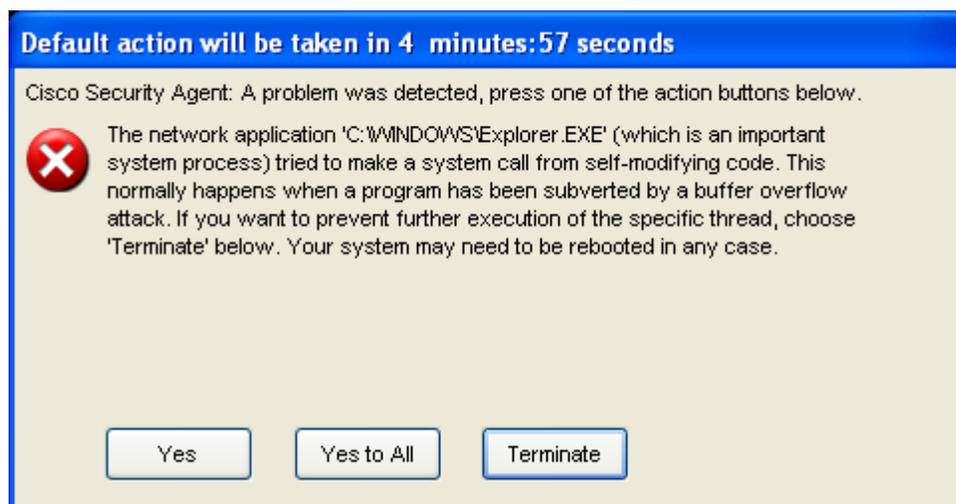


CSA in Action: Protection JPEG (GDI+) OVERFLOW

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

Cisco.com

The screenshot displays the Management Center for Cisco Security Agents (CSA) web interface. The browser window title is "Management Center for Cisco Security Agents - Microsoft Internet Explorer". The address bar shows "https://csamc/csamc/webadmin". The interface includes a navigation menu with options like "Monitor Systems", "Configuration", "Maintenance", "Reports", "Profiler", "Search", and "Help". A table of security events is visible, with columns for ID, Date/Time, Hostname, Severity, and Description. The events listed are:

ID	Date/Time	Hostname	Severity	Description
7324	5/4/2004 9:55:20 AM	XP-PRO-SP1A	Alert	TESTMODE: The application 'C:\WINDOWS\system32\8_up.exe' (as user NT AUTHORITY\SYSTEM) tried to call the function CreateThread("") from a buffer (the return address was 0x402058). The code at this address is '008d45f8 50565668 f51e4000 5656ffd7 4b75ee5f 5b56ff15 00504000 68b80b00'. This either happens when a program uses self-modifying code or when a program has been subverted by a buffer overflow attack. The program would have been terminated.
7323	5/4/2004 9:55:20 AM	XP-PRO-SP1A	Warning	TESTMODE: The process 'C:\WINDOWS\system32\8_up.exe' (as user NT AUTHORITY\SYSTEM) tried to open/create the file 'C:\WINDOWS\avserve.exe'. This would have caused the user to be prompted as to the action to take.
7322	5/4/2004 9:55:20 AM	XP-PRO-SP1A	Alert	TESTMODE: The program 'C:\WINDOWS\system32\8_up.exe' was downloaded from the network and is now trying to execute. This is an unusual event, but can happen during automated software installation. This would normally trigger a user query.
7321	5/4/2004 9:55:19 AM	XP-PRO-SP1A	Warning	TESTMODE: The process 'C:\WINDOWS\system32\ftp.exe' (as user NT AUTHORITY\SYSTEM) tried to open/create the file 'C:\WINDOWS\system32\8_up.exe'. This would have caused the user to be prompted as to the action to take.
7320	5/4/2004 9:55:17 AM	XP-PRO-SP1A	Alert	TESTMODE: The current application 'C:\WINDOWS\system32\lsass.exe' (as user NT AUTHORITY\SYSTEM) would not have been permitted to execute the new application 'C:\WINDOWS\system32\cmd.exe'.

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

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

Cisco.com

The screenshot shows the Management Center for Cisco Security Agents (CSA) web interface in Microsoft Internet Explorer. The browser address bar shows the URL: https://radams-storm/csamc/webadmin. The page title is "Management Center for Cisco Security Agents". The navigation menu includes "Monitor", "Systems", "Configuration", "Maintenance", "Reports", "Search", and "Help". The "Monitor" section is active, and the "Event Log" is displayed. There are 29 events, with a "change filter" button. The event log generation time is 6/6/2003 10:42:22 AM. The severity is Information - Emergency, and the host is All. The policy is All, and the events per page are 50. The event log table shows two entries:

#	Date	Host	Severity	Event
29	6/6/2003 10:40:59 AM	radams-w2ksp0	Warning	The program 'C:\Documents and Settings\win2k\Local Settings\Temporary Internet Files\Content.IE5\WO80SKOY\fizzer.exe' was recently downloaded and attempted to execute. The user was queried whether to allow this operation. The user chose 'Terminate'. Details Rule 97 Wizard Find Similar
28	6/6/2003 10:40:32 AM	radams-w2ksp0	Warning	The process 'C:\Program Files\Outlook Express\msimn.exe' (as user RADAMS-W2KSP0\win2k) tried to open/write the file 'C:\Documents and Settings\win2k\Local Settings\Temporary Internet Files\Content.IE5\WO80SKOY\fizzer.exe' and the user was queried. The user responded by choosing 'Yes'. Details Rule 99 Wizard Find Similar

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

CSA in Action: Protection Against BugBear

Cisco.com

The screenshot shows the Management Center for Cisco Security Agents (CSA) web interface in Microsoft Internet Explorer. The browser address bar shows the URL <https://radams-storm/csamc/webadmin>. The page title is "Management Center for Cisco Security Agents". The navigation menu includes "Monitor", "Systems", "Configuration", "Maintenance", "Reports", and "Search Help". The "Monitor" section is active, and the "Event Log" is displayed. The event log shows 60 events, with 11 displayed on this page. The event log generation time is 6/6/2003 3:08:35 PM. The severity is Information - Emergency, host is All, policy is All, and events per page is 50. The event log is sorted by "Latest" to "Earliest".

#	Date	Host	Severity	Event
60	6/6/2003 3:07:26 PM	radams-w2ksp0	Warning	The process 'C:\bugbear\102-6480315-2615331704426dd [1].pif' (as user RADAMS-W2KSP0\win2k) tried to open/create the file 'C:\WINNT\System32\Winkbj.exe' and the user was queried. The user responded by choosing 'No'. Details Rule 277 Wizard Find Similar
59	6/6/2003 3:06:37	radams-storm.example.com	Alert	The process '<remote application>' (as user RADAMS-STORM\win2k) tried to open/read the file 'C:\102-

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

CSA in Action: Protection Against Blaster

Cisco.com

The screenshot shows the Management Center for Cisco Security Agents web interface. The browser window title is "Management Center for Cisco Security Agents - Microsoft Internet Explorer". The address bar shows "https://radams-storm/csamc/webadmin". The page title is "Management Center for Cisco Security Agents". The navigation menu includes "Monitor Systems Configuration Maintenance Reports Profiler Search Help". The main content area displays a table of events for host "rob-xp-pro" on "8/13/2003". The events are sorted by "Latest" and "Earliest". The table has columns for "#", "Date", "Host", "Severity", and "Event".

#	Date	Host	Severity	Event
73	8/13/2003 4:18:13 PM	rob-xp-pro	Alert	TESTMODE: The program 'C:\WINDOWS\System32\msblast.exe' was downloaded from the network and is now trying to execute. This is an unusual event, but can happen during automated software installation. This would normally trigger a user query. Details Rule 97 Wizard Find Similar
72	8/13/2003 4:18:11 PM	rob-xp-pro	Warning	TESTMODE: The process 'C:\WINDOWS\System32\tftp.exe' (as user NT AUTHORITY\SYSTEM) tried to rename to the file 'C:\WINDOWS\system32\msblast.exe'. This would have caused the user to be prompted as to the action to take. Details Rule 277 Wizard Find Similar
71	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The current application 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) would not have been permitted to execute the new application 'C:\WINDOWS\System32\CMD.EXE'. Details Rule 287 Wizard Find Similar
70	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to open/read the file 'C:\WINDOWS\system32\cmd.exe'. This would have been denied. Details Rule 280 Wizard Find Similar
69	8/13/2003 4:18:00 PM	rob-xp-pro	Alert	TESTMODE: The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) tried to accept a TCP connection from 10.5.64.127 on port 4444. This would have been prevented. Details Rule 325 Wizard Find Similar

At the bottom of the interface, there is a status bar that says "No rule changes pending" and a "Generate rules" button. The user is logged in as "admin". The Windows taskbar at the bottom shows the Start button, several open applications including "CiscoWorks - M...", "C:\WINNT\System...", "Select C:\WIN...", and "Management...". The system clock shows "4:22 PM".

CSA in Action: Protection Against Slammer

Cisco.com

The screenshot shows the Management Center for Cisco Security Agents (CSA) web interface in Microsoft Internet Explorer. The browser address bar shows the URL `https://radams-storm/csamc/webadmin`. The page title is "Management Center for Cisco Security Agents". The navigation menu includes "Monitor Systems Configuration Maintenance Reports Search Help". The current view is "Monitor > Event Log".

There is 1 event displayed. The event log generation time is 1/31/2003 11:02:45 AM. The severity is Information - Emergency. The host is All, the policy is All, and the rule is 153. The number of events per page is 50.

#	Date	Host	Severity	Event
1	1/31/2003 10:57:15 AM	stormserver	Warning	The application 'C:\Program Files\Microsoft SQL Server\MSSQL\Binn\sqlservr.exe' (as user NT AUTHORITY\SYSTEM) tried to call the function LoadLibraryA from a buffer (the return address was 0x38c3d457). The code at this address is '6873656e 64be1810 ae428d45 d450ff16 508d45e0 508d45f0 50ff1650 be1010ae'. 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 'Terminate'. Details Rule 153 Find Similar

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