

Blocking CodeMeter Run Time Server Vulnerabilities – Windows 7

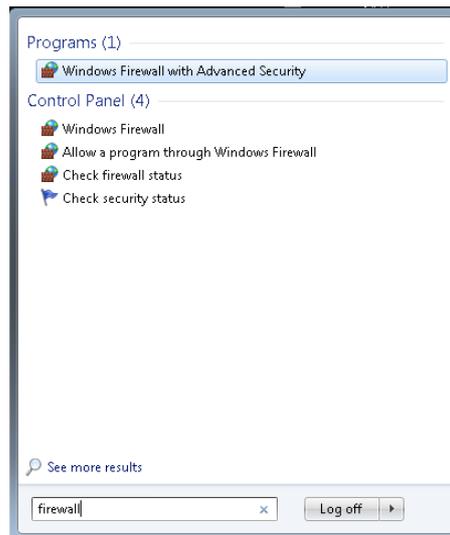
Purpose

The following instructions are to be used to mitigate the risk posed by the vulnerabilities in the Code Meter Runtime Server on systems running LAS-X, LMD and Paula.

Instructions

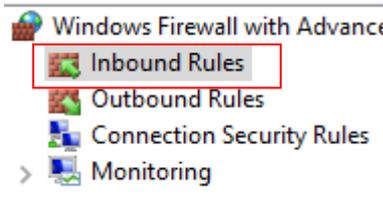
Login to the workstation running the product.

Click on the start menu and  and type firewall.



Select the  **Windows Firewall with Advanced Security** from the menu.

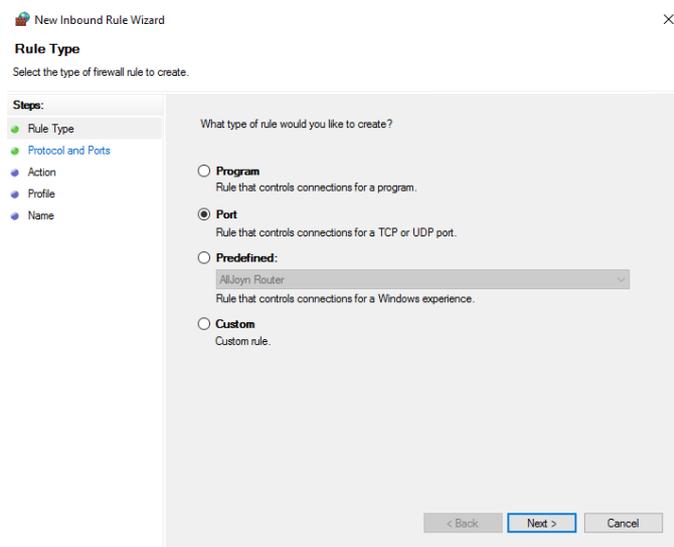
From the new windows that appears select the option „Inbound Rules“ as indicated below.



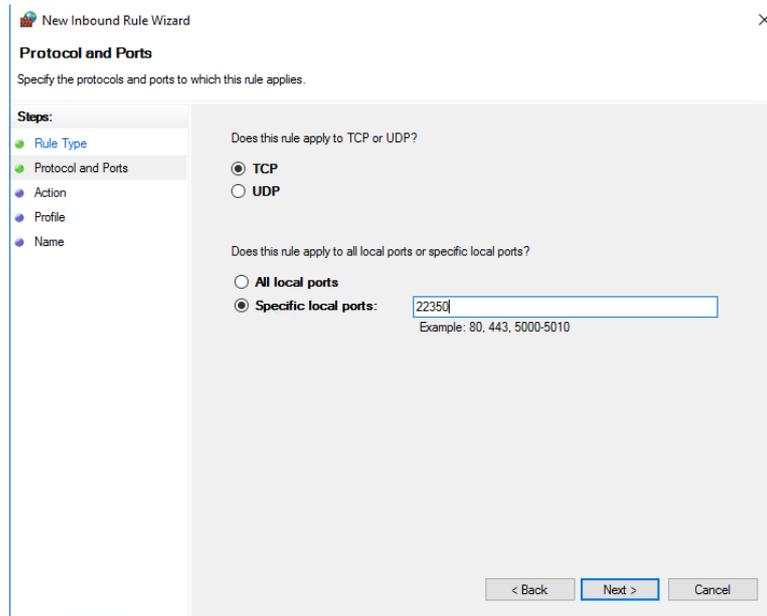
Then select the option New Rule...



In the dialogue that appears Select the option Port and press the next button.

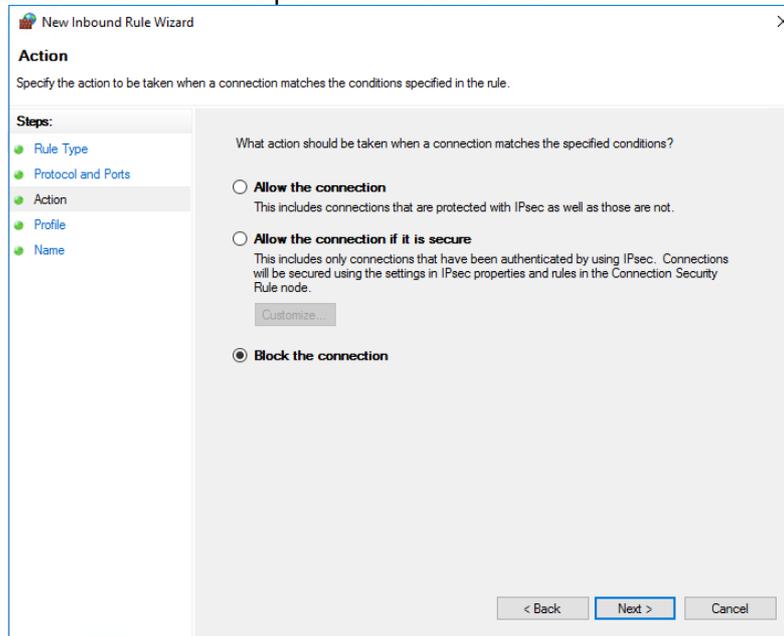


In the Specified Local Ports enter the port 22350 and press the next button.



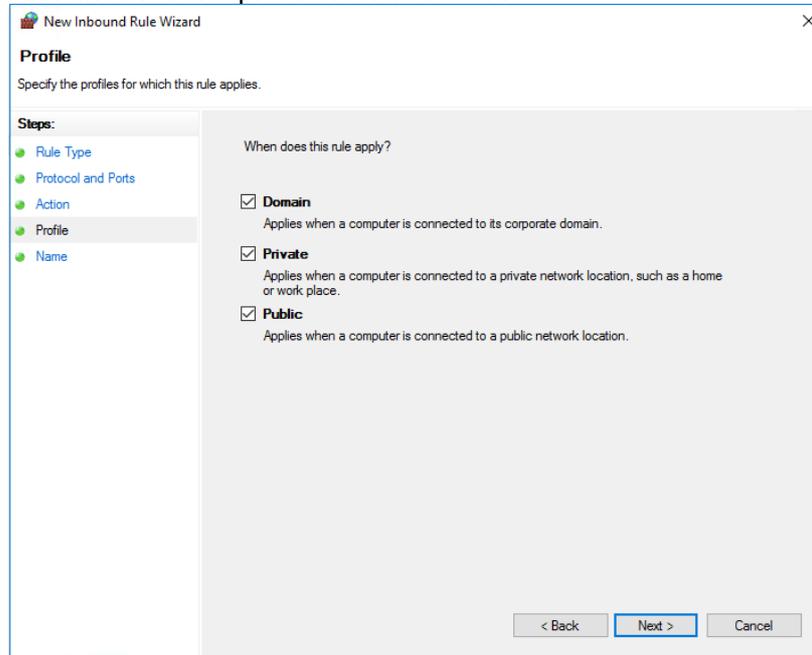
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps' pane lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text input field for 'Specific local ports' contains '22350' and has an example 'Example: 80, 443, 5000-5010' below it. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Select the action Block Connection and press the next button.



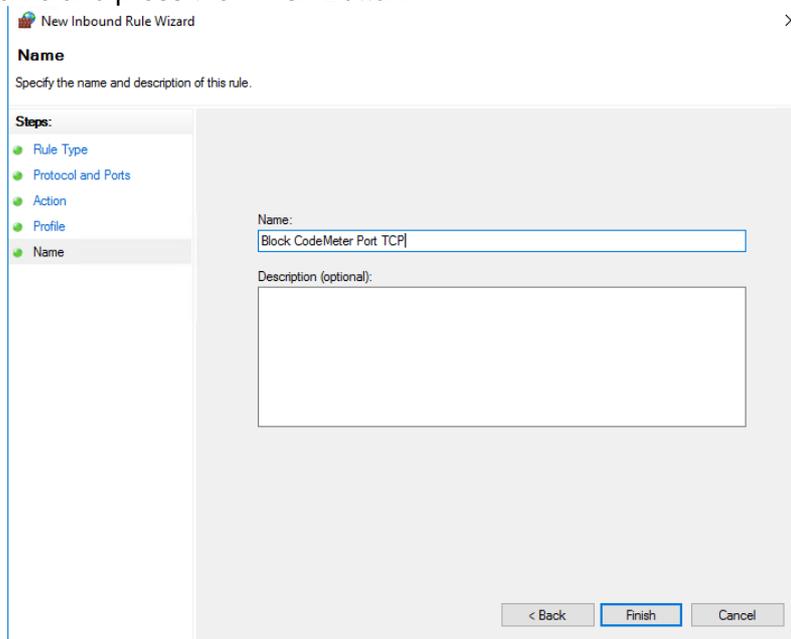
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps' pane lists: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (with subtext 'This includes connections that are protected with IPsec as well as those are not.'), 'Allow the connection if it is secure' (with subtext 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button), and 'Block the connection' (selected). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Ensure all options are checked and press the next button.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Give the Rule a name and press the Finish Button.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'Block CodeMeter Port TCP'. Below it is a 'Description (optional):' label followed by a larger empty text box. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'.

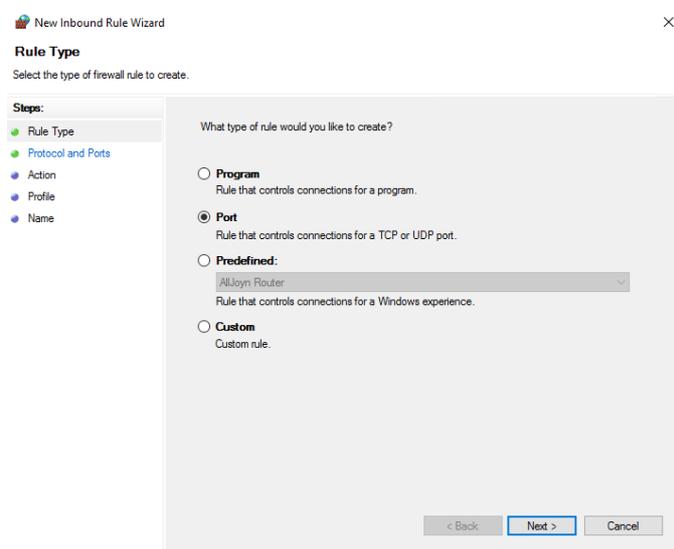
Page 5/8

Now repeat the process for UDP

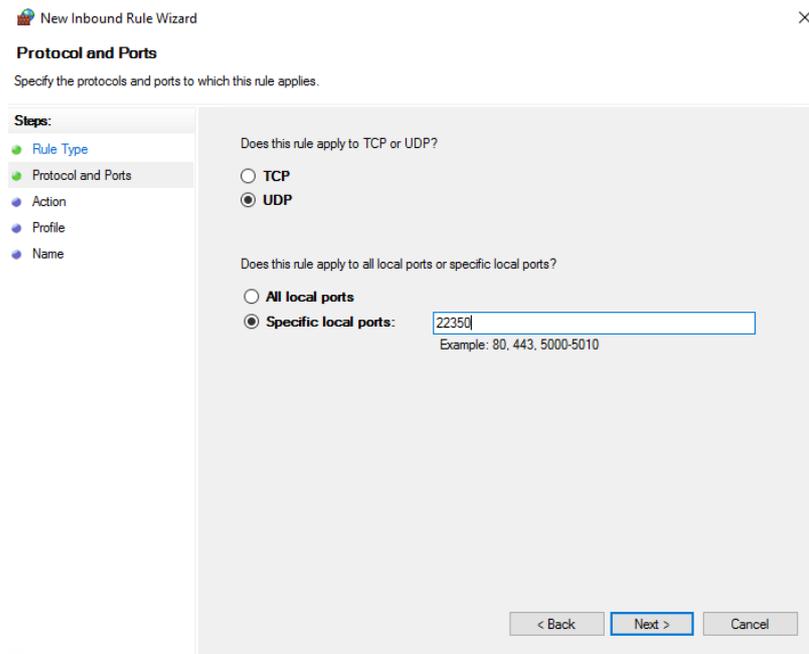
Then select the option New Rule...



In the dialogue that appears Select the option Port and press the next button.

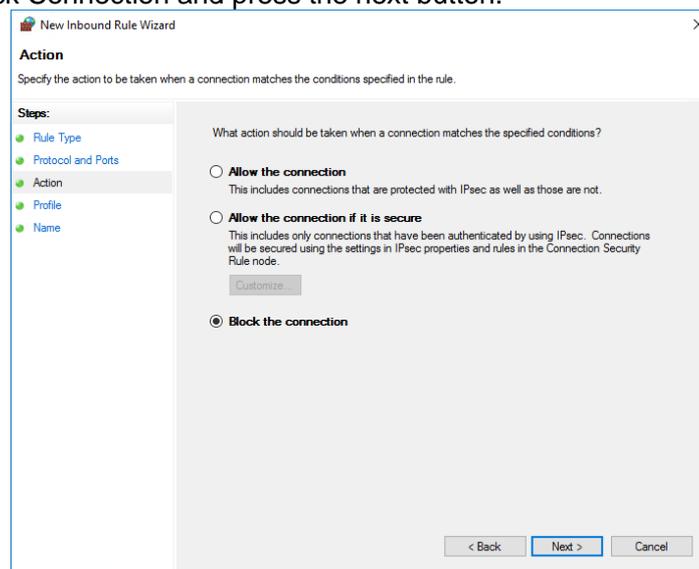


Select the option UDP and in the Specified Local Ports enter the port 22350 and press the next button.



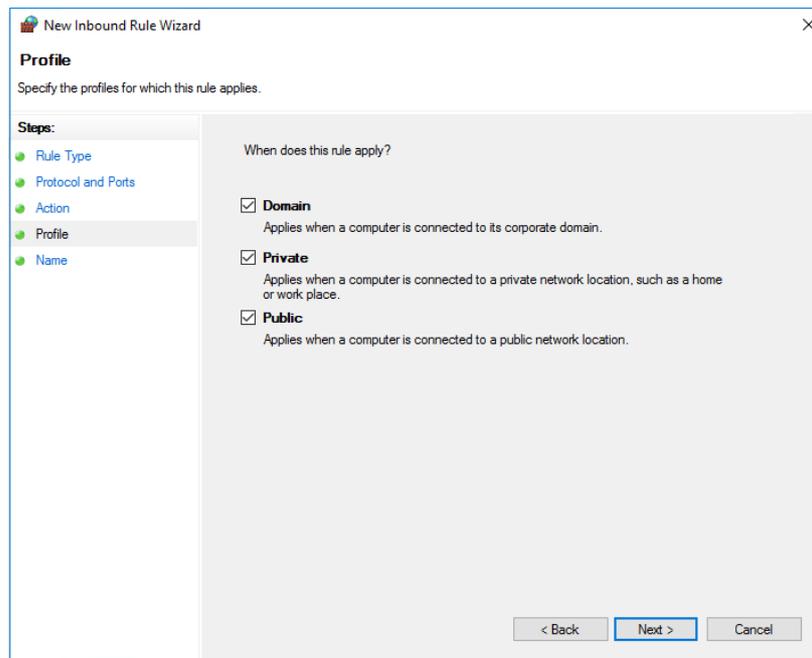
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Protocol and Ports' selected. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' and 'UDP' (selected), and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for 'All local ports' and 'Specific local ports:' (selected). Below the second question is a text input field containing '22350' and an example 'Example: 80, 443, 5000-5010'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Select the action Block Connection and press the next button.



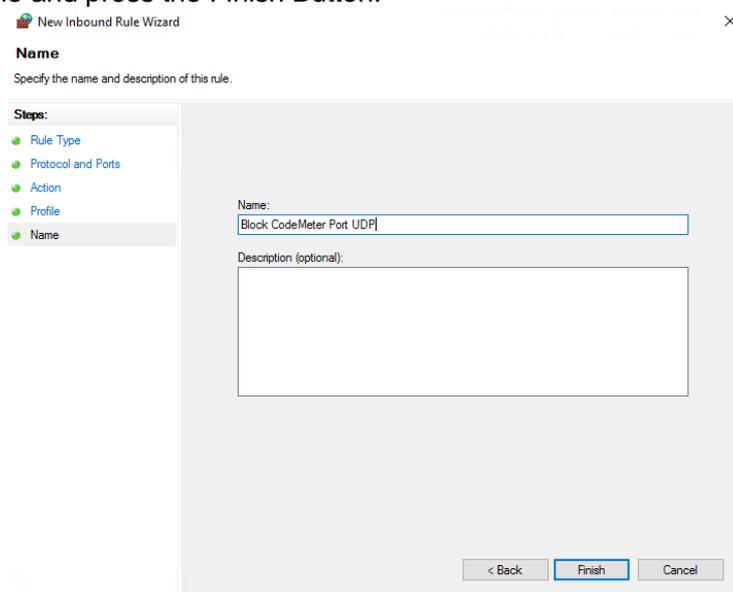
The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Inbound Rule Wizard' with a close button. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Action' selected. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (with subtext 'This includes connections that are protected with IPsec as well as those are not.'), 'Allow the connection if it is secure' (with subtext 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button), and 'Block the connection' (selected). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Ensure all options are checked and press the next button.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Profile' step is currently selected. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Give the Rule a name and press the Finish Button.



The screenshot shows the 'New Inbound Rule Wizard' dialog box, specifically the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list shows 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The 'Name' step is currently selected. The main area has a 'Name:' label followed by a text input field containing 'Block CodeMeter Port UDP'. Below it is a 'Description (optional):' label followed by a large empty text area. At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

You should now see in the list of inbound rules the new rules

Inbound Rules													
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Auth
 Block CodeMeter Port UDP		All	Yes	Block	No	Any	Any	Any	UDP	22350	Any	Any	Any
 Block CodeMeter Port TCP		All	Yes	Block	No	Any	Any	Any	TCP	22350	Any	Any	Any