

## **Problem Description**

A recently published Cisco NAC rule contained a bug that may result in a loss of service for NAC Servers (Clean Access Servers or CAS). Customers with NAC Managers (Clean Access Managers or CAM) which updated their Cisco Updates rule-sets between 3:15AM PST 11/11/2008 and 11:15AM PST 11/11/2008 are affected and subsequent updates will not be downloaded. The affected version of the rule is OS Detection Fingerprint Version 7.

By default a NAC Manager installed within a customer environment will automatically poll Cisco Updates for Operating System detection fingerprinting.

Note: 'OS Detection Fingerprint' is referred to as 'OSDF' for the remainder of this document. NAC Manager and CAM as well as NAC Server and CAS are synonymous and are used interchangeably throughout this document.

## **Background**

OSDF version 7 has a software bug that may result in a loss of service for NAC Servers. This version has been removed from the update server.

This documentation is intended to be a complete step-by-step procedure for repairing any impacted OSDF v7 NAC Appliances. Please contact Cisco Technical Assistance Center if you experience anything not covered by this procedure.

This field notice affects only customers with OS Detection Fingerprint (OSDF) Version 7 on their NAC Managers. Customers with OSDF Version 6 and prior or Version 8 and later on their NAC Managers are not affected.

## **Problem Symptom**

- a) A NAC Manager which downloads OSDF version 7 will subsequently stop receiving new rules and checks published via Cisco Updates.
- b) A new NAC Server added to the NAC Manager with OSDF version 7 will not be displayed in the NAC Manager UI.
- c) Any NAC Server that disconnects from the NAC Manager with OSDF version 7 cannot be re-connected.
- d) A 503 Error appears and blocks HTTP access to the NAC Manager UI if the NAC Manager with OSDF version 7 is in High Availability mode and fails over.
- e) This issue affects all releases of Cisco NAC Appliance Software (Cisco Clean Access Software).

## Problem Verification

Please verify the version of OSDF currently installed on your NAC Manager whether you're experiencing any of the above symptoms or not. Verification can be done through a standard web browser and is not business impacting.

Verification steps:

1. Log into NAC Manager interface via standard web browser
2. Navigate to **Device Management > Clean Access > Updates > Summary**
3. Compare your screen to the screen below. If OS Detection fingerprint: 7 is displayed, your system requires repair. The remediation steps required **IS** business impacting. Cisco recommends a scheduled maintenance window before proceeding.

Device Management > Clean Access

The screenshot shows the 'Clean Access Agent' tab in the NAC Manager interface. The breadcrumb trail is 'Device Management > Clean Access > Updates > Summary'. The 'Summary' link is highlighted in yellow. Below the breadcrumb, there are tabs for 'Certified Devices', 'General Setup', 'Network Scanner', 'Clean Access Agent', and 'Updates'. The 'Clean Access Agent' tab is active. Under the heading 'Current Versions of Updates', there are two columns of information. The first column lists: 'Cisco Checks & Rules: 44594', 'Supported AV/AS Product List: 67', 'Default Host Policies: 3', 'Default L2 Policies: 2', 'OS Detection Fingerprint: 7' (highlighted with a red box), and 'Supported Out-of-Band Switch OIDs: 9'. The second column lists: 'Windows Clean Access Agent Patch: 4.1.3.0', 'Macintosh Clean Access Agent: 4.1.3.0', 'Cisco NAC Web Agent: 4.1.3.9', 'Cisco NAC Web Agent Facilitator (ActiveX/Applet): 2.0.1.0 / 2.0.0.0', and 'L3 MAC Address Detection (ActiveX/Applet): 2.1.0.0 / 2.1.0.1'.

Certified Devices	General Setup	Network Scanner	Clean Access Agent	Updates
Summary	Update	HTTP Settings		

**Current Versions of Updates**

Cisco Checks & Rules: 44594	Windows Clean Access Agent Patch: 4.1.3.0
Supported AV/AS Product List: 67	Macintosh Clean Access Agent: 4.1.3.0
Default Host Policies: 3	Cisco NAC Web Agent: 4.1.3.9
Default L2 Policies: 2	Cisco NAC Web Agent Facilitator (ActiveX/Applet): 2.0.1.0 / 2.0.0.0
OS Detection Fingerprint: 7	L3 MAC Address Detection (ActiveX/Applet): 2.1.0.0 / 2.1.0.1
Supported Out-of-Band Switch OIDs: 9	

4. If your current OSDF update lists any version other than 7 your NAC solution is not impacted. No further action is required.

## Resolution

ATTENTION: This resolution involves restarting your NAC system and should only be attempted during a scheduled maintenance window. The expected resolution time is roughly 20 minutes for NAC Manager and NAC Server pair. For each additional NAC Server pair add 5 minutes. Please do not begin any part of the following resolution procedure until you have appropriately planned for the expected down time.

CCO login will be required to access the download. Please have all of your service contract information on hand to begin. You can find additional information on Service Contracts in the footnote section of this document. If at any time you have difficulty with this procedure please open a service request with Cisco Technical Assistance center:

<http://tools.cisco.com/ServiceRequestTool/create/launch.do>

## Preparation

1. From your workstation please close all open applications and download the file:

**"Patch-CSCsv69462.tar.gz"**

From Cisco Connection Online location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches>

2. Upload the patch file in to the /store directory on each NAC Manager in your environment using SFTP/SCP as per Cisco's normal NAC patching process. Please note your NAC Console administrative credentials will be required to complete the copy. Follow the instructions for your SSH capable file transfer utility for the necessary steps to provide them.

3. SSH into each of your NAC Managers, change directory to /store and extract the contents of the downloaded patch file by running the following commands:

**cd /store**

4. Verify each of your NAC units has properly copied by entering the following command at the /store directory:

**ls**

You should see Patch-CSCsv69462.tar.gz listed under the /store directory

5. Extract the contents of the downloaded patch file by running the following command:

**tar xvzf Patch-CSCsv69462.tar.gz**

```
[root@cam-p ~]#  
[root@cam-p ~]# cd /store/  
[root@cam-p store]# ls  
Patch-CSCsv69462.tar.gz  
[root@cam-p store]# tar xvzf Patch-CSCsv69462.tar.gz  
CAMSigPatch.sh  
[root@cam-p store]# █
```

I

This will extract one file - CAMSigPatch.sh in the /store folder as shown above.

6. Verify that the file has been properly extracted to the /store directory with the following command:

```
ls
```

You should see CAMSigPatch.sh listed under the /store directory.

If you do not see this file please verify that steps 1-5 in this section completed properly.

### **NAC Manager (CAM) Repair:**

1. SSH to the NAC Manager (Active CAM for HA setup) .

Use the following command to verify that you are logged into the Active NAC Manager:

```
/perfigo/common/bin/fostate.sh
```

For the Active NAC Manager the command should respond with:

My node is active, peer node is standby

2. Change directory to /store and use the following commands to start the CAMSigPatch.sh script on the Active NAC Manager from the /store folder as follows:

```
cd /store
```

```
./CAMSigPatch.sh
```

3. Executing the above command returns one of the following:

If the NAC Manager was not impacted you will receive the following message:

**"This CAM is not affected by the bad OS fingerprint signature!"**

No other action is required for this appliance. Please continue to check remaining NAC components.

If your NAC Manager was impacted you will receive the following message:

**"This CAM is affected by the bad OS fingerprint!"**

**Do you want to continue to clean the bad OS fingerprint on this CAM? (y/n)? [y]?"**

Note: If you do not see either message please verify that steps 1-6 in the Preparation section above completed properly.

4. Enter 'y' at the prompt to continue, enter 'n' to abort this procedure.

5. The console will display '**Cleaning successfully completed**' following execution of the script and cleanup of the NAC Manager.

Expected time to clean is typically less than one minute. If after ten minutes you have not received a success message or you receive any other message back please contact the Cisco Technical Assistance Center.

**Note: Do not restart either the Active or Standby Manager at this time. You must first complete NAC Server Repair before initializing a restart.**

6. Continue to step 7 if you are running a redundant (HA) configuration. Skip to NAC Server Cleaning if you only have a single NAC Manager.

7. SSH to the Standby NAC Manager.

Use the following command to verify that you are logged into the Standby NAC Manager:

```
/perfigo/common/bin/fostate.sh
```

The command should respond with:

My node is standby, peer node is active

8. Change directory to /store and use the following commands to start the CAMSigPatch.sh script on the Standby NAC Manager from the /store folder as follows:

```
cd /store  
./CAMSigPatch.sh
```

9. Executing the above command returns one of the following:

If the NAC Manager was not impacted you will receive the following message:

**"This CAM is not affected by the bad OS fingerprint signature!"**

No other action is required for this appliance. Please continue to check remaining NAC components.

If the NAC Manager was impacted you will receive the following message:

**"This CAM is affected by the bad OS fingerprint!**

**Do you want to continue to clean the bad OS fingerprint on this CAM? (y/n)? [y]?"**

Note: If you do not see either message please verify that steps 1-6 in the Preparation section above completed properly.

10. Enter 'y' at the prompt to continue, enter 'n' to abort this procedure.

11. The console will display '**Cleaning successfully completed**' following execution of the script and cleanup of the NAC Manager.

Expected time to clean is typically less than one minute. If after ten minutes you have not received a success message or you receive any other message back please contact the Cisco Technical Assistance Center.

**Note: Do not reboot the Standby NAC Manager at this time.**

12. Continue to NAC Server Repair

### **NAC Server (CAS) Repair:**

Please ensure that you have completed the previous steps for NAC Manager (CAM) Recovery before you proceed

1. SSH to the Active NAC Server.

Use the following command to verify that you are logged into the Active NAC Server:

**/perfigo/common/bin/fostate.sh**

The command should respond with:

My node is active, peer node is standby

2. Reboot the active NAC Server by executing the following command

**service perfigo reboot**

Wait 5 to 10 minutes for the NAC Server to complete the boot cycle. This will become standby NAC server. Make sure it becomes standby by checking via the command

**/perfigo/common/bin/fostate.sh.**

The command should respond with:

My node is standby, peer node is active

3. Now reboot the new active NAC Server. Use the following command to verify that you are logged into the Active NAC Server:

**/perfigo/common/bin/fostate.sh**

The command should respond with:

My node is active, peer node is standby

4. Reboot the active NAC Server by executing the following command

**service perfigo reboot**

Wait 5 to 10 minutes for the NAC Server to complete the boot cycle. This will become standby NAC server. Make sure it becomes standby by checking via the command

**/perfigo/common/bin/fostate.sh.**

The command should respond with:

My node is standby, peer node is active

4. Repeat steps 1-4 for each NAC Server pair in the environment.

## Final Steps:

Note: For a Standalone NAC Manager setup, proceed directly to step 3

1. SSH to the Standby NAC Manager.

Use the following command to verify that you are logged into the Standby NAC Manager:

**/perfigo/common/bin/fostate.sh**

The command should respond with:

My node is standby, peer node is active

2. Execute the **service perfigo stop** command

3. SSH to the active NAC Manager and use the following command to verify the standby peer is dead.

**/perfigo/common/bin/fostate.sh**

The command should respond with:

My node is active, peer node is dead

4. Restart the active NAC Manager by issuing the following command:

**service perfigo reboot**

Wait 5 to 10 minutes for the NAC Manager to complete the boot cycle.

5. Log into the Active NAC Manager interface with a standard web browser.

6. Navigate to **Device Management > Clean Access > Updates > Summary**

The OS Detection Fingerprint version should show **6** as below:

Certified Devices	General Setup	Network Scanner	Clean Access Agent	Updates
Summary	Update	HTTP Settings		

**Current Versions of Updates**

Cisco Checks & Rules: <b>44594</b>	Windows Clean Access Agent Patch: <b>4.1.3.0</b>
Supported AV/AS Product List: <b>67</b>	Macintosh Clean Access Agent: <b>4.1.3.0</b>
Default Host Policies: <b>3</b>	Cisco NAC Web Agent: <b>4.1.3.9</b>
Default L2 Policies: <b>2</b>	Cisco NAC Web Agent Facilitator (ActiveX/Applet): <b>2.0.1.0 / 2.0.0.0</b>
OS Detection Fingerprint: <b>6</b>	L3 MAC Address Detection (ActiveX/Applet): <b>2.1.0.0 / 2.1.0.1</b>
Supported Out-of-Band Switch OIDs: <b>9</b>	

7. Navigate to **Device Management > Clean Access > Updates > Update**. Click on the update button to get the latest update. This may take up to 10 minutes.

8. Navigate to **Device Management > Clean Access > Updates > Summary**. Confirm the OS Detection Fingerprint id is set to **8**.

Certified Devices	General Setup	Network Scanner	Clean Access Agent	Updates
Summary	Update	HTTP Settings		

**Current Versions of Updates**

Cisco Checks & Rules: <b>44594</b>	Windows Clean Access Agent Patch: <b>4.1.3.0</b>
Supported AV/AS Product List: <b>67</b>	Macintosh Clean Access Agent: <b>4.1.3.0</b>
Default Host Policies: <b>3</b>	Cisco NAC Web Agent: <b>4.1.3.9</b>
Default L2 Policies: <b>2</b>	Cisco NAC Web Agent Facilitator (ActiveX/Applet): <b>2.0.1.0 / 2.0.0.0</b>
OS Detection Fingerprint: <b>8</b>	L3 MAC Address Detection (ActiveX/Applet): <b>2.1.0.0 / 2.1.0.1</b>
Supported Out-of-Band Switch OIDs: <b>9</b>	

9. If your current OSDF update lists any version other than **8** please verify all previous steps have been completed properly.

10. SSH to the **Standby** NAC Manager and execute the following command to reinitialize the NAC Manager:

**service perfigo start**

## Final Verification

1. Verify that all NAC Appliances are in their expected HA state. SSH to each and execute the following command:











/perfigo/common/bin/fostate.sh

2. Log into the Active NAC Manager interface with a standard web browser.
3. Navigate to **Device Management>CCA Servers**
4. Verify management connectivity of all NAC Servers from the NAC Manager UI by clicking on the 'Manage' button listed next to each of the listed NAC Servers.

Device Management > Clean Access Servers

List of Servers

New Server

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.242.130	Virtual Gateway	ISR	Connected				
10.201.217.95 [10.201.217.97]	Real-IP Gateway	CAS3	Connected				

5. If the NAC Server is properly connected clicking the 'Manage' button will display the Server Properties screen as shown below:

Device Management > Clean Access Servers > 172.23.117.26

Status	Network	Filter	Advanced	Authentication	Misc
Module			Status		

6. If you are not able to see the property screen as shown above, then go to back to **NAC Server (CAS) Repair** section of this document and verify the process again

## Footnote

### Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

### Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact

that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

### **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

+1 800 553 2447 (toll free from within North America)  
+1 408 526 7209 (toll call from anywhere in the world)  
e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to

[http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.