Product Notice #332

Installing May 2018 Windows Server 2012 R2 Update

on Cloud Connector Edition (CCE)

Overview

This Product Notice describes the issues and corrective action for installing the May 2018 Windows Server 2012 R2 update on the CCE.

The May 2018 Windows update includes an update for the Credential Security Support Provider protocol (CredSSP), which is an authentication provider that processes authentication requests for other applications.

A remote code execution vulnerability exists in unpatched versions of CredSSP. A potential hacker, who successfully exploits this vulnerability, could relay user credentials to execute code on the target system. Any application that depends on CredSSP for authentication may be vulnerable to this type of attack.

The May 2018 security update addresses the vulnerability by correcting how CredSSP validates requests during the authentication process. The May 2018 security update changes the default setting from **Vulnerable** to **Mitigated**.

For more information about the vulnerability, refer to CVE-2018-0886.

How the Update Affects the CCE

For CCE Installations

The CCE installation may fail with the following error message or similar message:

"Connecting to remote server 192.168.213.3 failed with the following error message: The request is not supported. For more information, see the About_Remote_Troubleshooting Help topic."

This error may occur after installing the May 2018 security update on the CCE Host, and if the CCE Master VHDX was created before May 2018.

For Already Installed CCEs

Already installed CCEs may have encountered the following:

- Communication issues between the Host and the virtual machines
- Future CCE upgrades may have the same error message as shown above (for CCE Installations) because the CCE upgrade will re-install the CCE.

Corrective Action

For CCE Installations

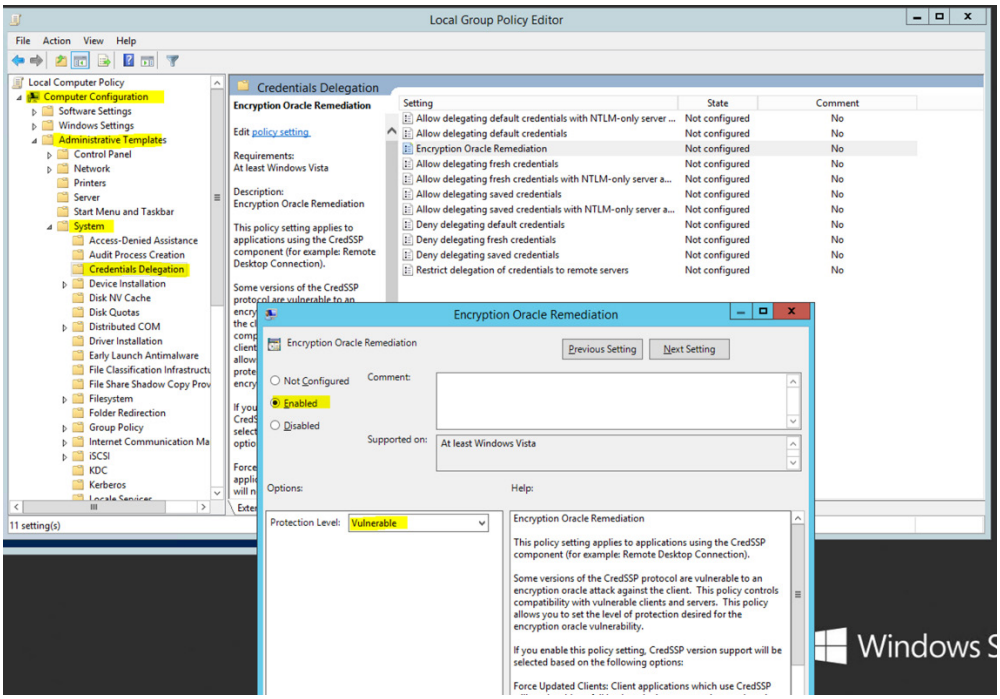
There are two options to fix these issues:

- Update the CCE with the latest VHDX Master (see below) and update the CCE Host with the latest Windows security updates.

Note: For security reasons, this is the recommended option.

- Use the following workaround to change the Host policy:

1. Open the Local Group Policy Editor and navigate to **Computer Configuration** > **Administrative Templates** > **System** > **Credentials Delegation**.
2. Under 'Encryption Oracle Remediation', click the **Enabled** option.
3. From the 'Protection Level' drop-down list, select **Vulnerable**.



For Already Installed CCEs

There are two options to fix these issues:

- Update the VHDX and Operating Systems by doing the following:

    1. Update the CCE with the latest VHDX Master (see below).
    2. Perform the above workaround (See Corrective Action for CCE Installations) to change the Host policy on the CCE Host.
    3. Update the CCE Host and the four CCE Virtual Machines with the instructions explained in CVE-2018-0886.
    4. On the Host, change the 'Host Policy' field to **Not Configure**.

Note: If your CCE is set to perform automatic Operating System updates and all Operating Systems (Host and the four Virtual Machines) were already updated with the March KB4088876 (Monthly Rollup) or a newer Monthly Rollup, skip **Steps 2-4** above (for Already Installed CCEs).

Note: For security reasons, this is the recommended option. This option requires a restart of the CCE Host and virtual machines.

- Perform the workaround only, to change the Host policy.

To Update the CCE with the Latest VHDX Master

Update the production CCEs and the new CCEs that have arrived with the old CCE version, with the updated VHDX file that is used as the master VHDX to prepare the four CCE VMs.

Note: The CCE auto-update feature will only update the wizard and the CCE bits, but not the VHDX master.

1. Download the latest VHDX from: https://downloads-audiocodes.s3.amazonaws.com/Download/AC_CCE_VHDX.html
2. Copy the VHDX to the following places:
   a. For all CCEs in the site, copy to **D:\CCESources\Bits\VHD**.
   b. Copy and unzip the VHDX file to the site directory (once per site) at **<site directory>\Bits\VHD**.
3. Run the *Get-CcSiteDirectory* PowerShell script on the CCE Host, to get the site directory path.
4. Copy the VHDX to the CCE Recovery USB at **<USB Root>\CCESources\Bits\VHD.** It may be used to re-image the CCE in the future.