Intel Action Alert AA-0002-1

5200 NE Elam Young Parkway
Hillsboro, OR 97124

July, 2012

Intel Hybrid Cloud Security Update

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice. The Intel products described herein may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Products Affected

Intel® Hybrid Cloud platform 2.5, 3.0, 3.1, and 3.1.1

Description

A Citrix XenServer* vulnerability has recently been reported by Citrix* that could pose a security risk to any system using XenServer Hypervisor, including the Intel Hybrid Cloud platform which uses Citrix XenServer* VMM as the virtualization platform.

Root Cause

Some 64-bit operating systems and virtualization software running on Intel CPU hardware are vulnerable to a local privilege escalation attack. The vulnerability may be exploited for local privilege escalation or a guest-to-host virtual machine escape.

Intel processors are functioning as per their documented specifications. However, software that fails to take the Intel-specific SYSRET behavior into account may be vulnerable.

Corrective Action / Resolution

Hotfixes have been released by Citrix* that address these issues in all supported versions and update levels of Citrix XenServer*. Intel adapted this Citrix* update for deployment onto the Intel Hybrid Cloud (IHC) platform. Intel strongly recommends that customers using Intel Hybrid Cloud apply the update from Intel. It will take an estimated 10-15 minutes to complete this update.

Pre-requisite

Prior to installing the update, **ensure all software virtual machines are shut down**, Intel Hybrid Cloud Server Manager is updated to latest version, and firewall rules are configured.

- Shut down all software virtual machines. (Physical server restart is not required)
- For IHC platforms 3.0 or newer, upgrade the Hybrid Cloud server manager to version 3.5. Download link: http://downloadcenter.intel.com/Detail_Desc.aspx?ProductID=3393&DwnldID=21529&lang=eng&iid=dc_rss
- Firewall settings:
  - Outbound TCP/IP ports:
    - 80/443 – Intel download center (Http/Https)
  - Inbound TCP/IP ports if applying update remotely:
    - 64440 – Hybrid Cloud Server Manager console
    - 65222 – Hybrid Cloud Server Manager script tool
  - Web security:
    - Do not filter/restrict access to Citrix* download center:
      - https://support.citrix.com
      - http://support.citrix.com

Recommended Customer Action

Customers are advised to follow the instructions below to successfully apply the update. The update can be applied remotely or locally.

Option #1: For servers running Intel Hybrid Cloud Software Stack 3.0 or newer

1. Login to the Intel Hybrid Cloud management portal (https://hybridcloud.intel.com), select the Patch button from the left-hand navigation pane, select the relevant Intel Hybrid Cloud server (checkbox), and select Confirm to apply the patch (patch version 3.1.2).
2. Using ixe command line tool, do a "sync-with-portal" to ensure the patch information is sent to server immediately
   `ixe.exe –h <ip_address> -u admin –p <password> -o sync-with-portal`
   (**`ixe.exe`** is generally located at **`C:\Program Files (x86)\HybridCloudServerManager`**)
3. Connect to the server via Intel Hybrid Cloud server manager, there will be ticker message displayed on Dashboard on the availability of 3.1.2 patch. Authorize the patch via Controls → Maintenance → Upgrade. Patch will be installed.

Option #2: For server running Intel Hybrid Cloud Software Stack 2.5 (or cannot use the upgrade from the Intel Hybrid Cloud Management Portal as described in Option #1)

1. Download the **LM_critical_xen_patch.zip** file to a local management computer (laptop/workstation)
   - http://downloadmirror.intel.com/21530/eng/LM_critical_xen_patch.zip
   - Preferably, download/copy to **`C:\Program Files (x86)\HybridCloudServerManager`**
   - Extract the contents of the zip file (**LM_critical_xen_patch.pl**) to **`C:\Program Files (x86)\HybridCloudServerManager`**
2. Execute IXE command ("upload-system-scripts") to upload the script to the IHC System

```
ixe.exe –h <ip_address> -u admin –p <password> -o upload-system-scripts
"LM_critical_xen_patch.pl"
```
(**ixe.exe** is generally located at **C:\Program Files (x86)\HybridCloudServerManager**)

3. Once the script is uploaded to the IHC system, it will appear in the Scripts tab (in Intel Hybrid Cloud server manager → Controls → Scripts) as **"Critical Security Patch Update".** Select this option.

4. Once the Patch has been applied successfully, do a software reset (Hybrid Cloud server manager → Maintenance → Software Reset)

5. Review the following screenshots for further instructions.

   <u>Important:</u>
   o Do not close the UI or move to another tab until the patch process is completed.
   o If there is any network/power failures please repeat steps 3-4 again.
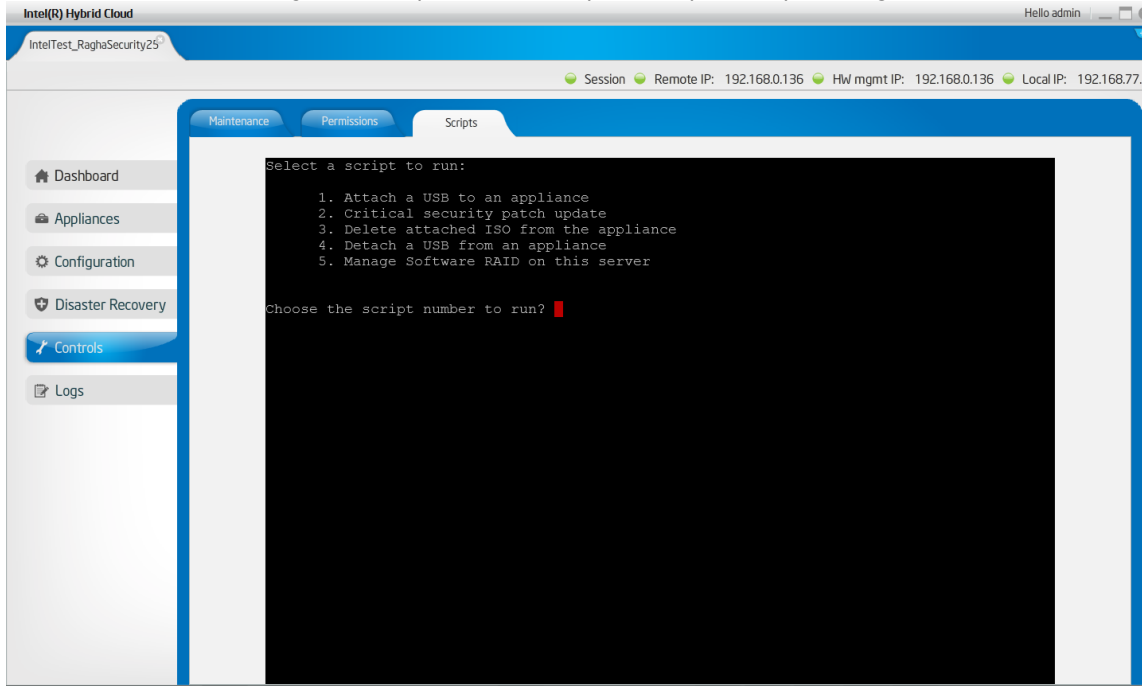
Once selected, the patch will start the download and the installation will be complete. There will be a confirmation message saying "Patch Applied successfully".

Note: During the patch download/install process do not move to other tab or close the UI.
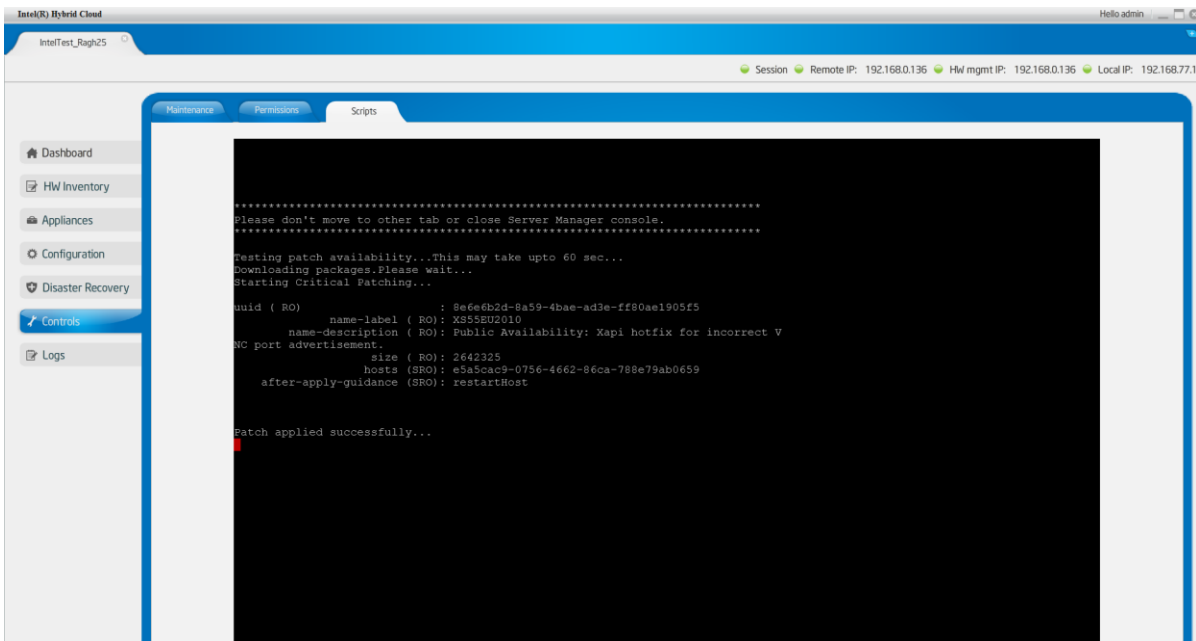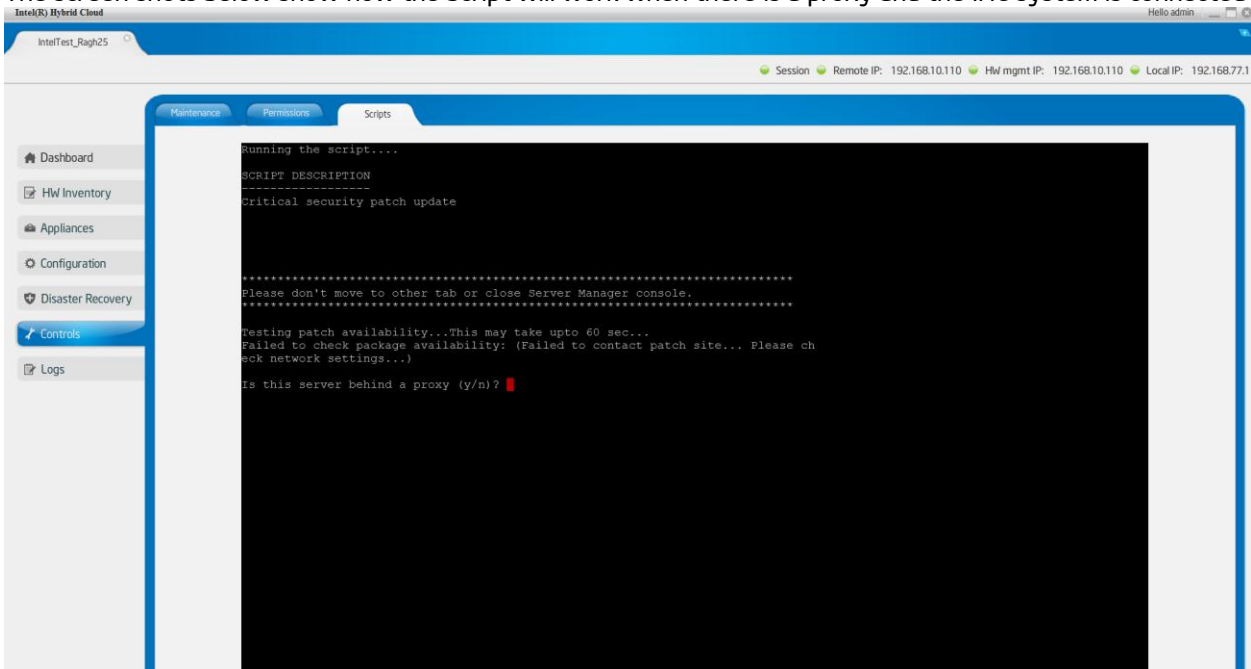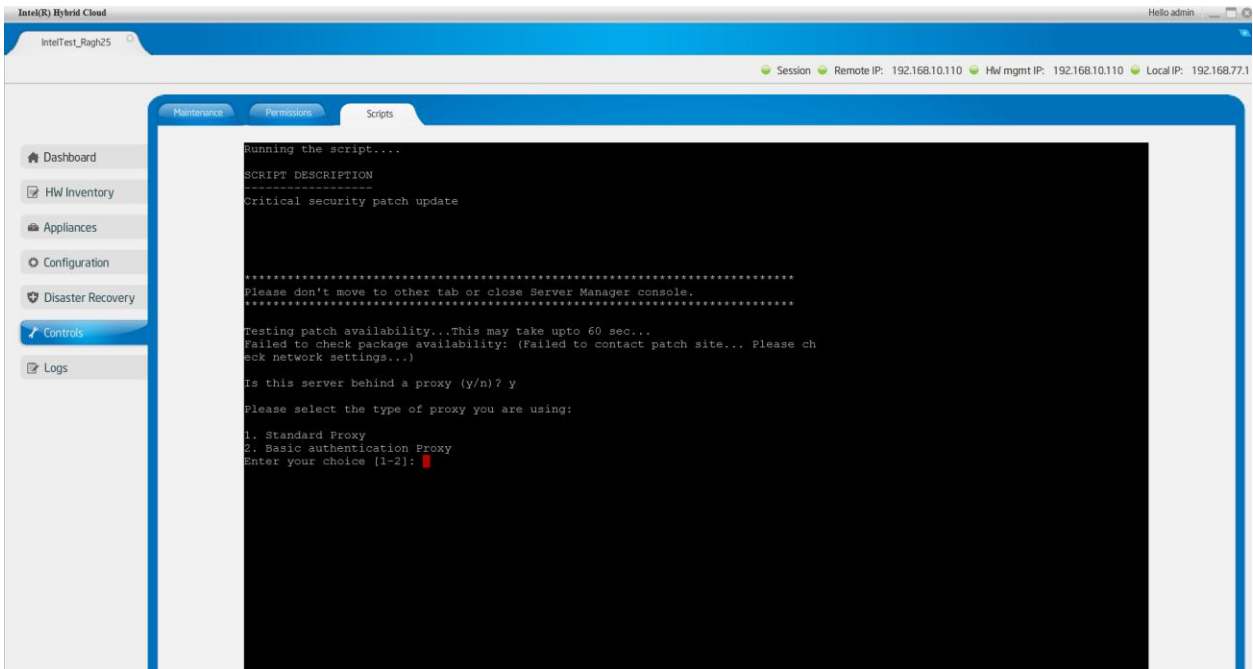
Proxy Settings

If the Server is behind a proxy, then the script will ask for the Proxy Server IP.
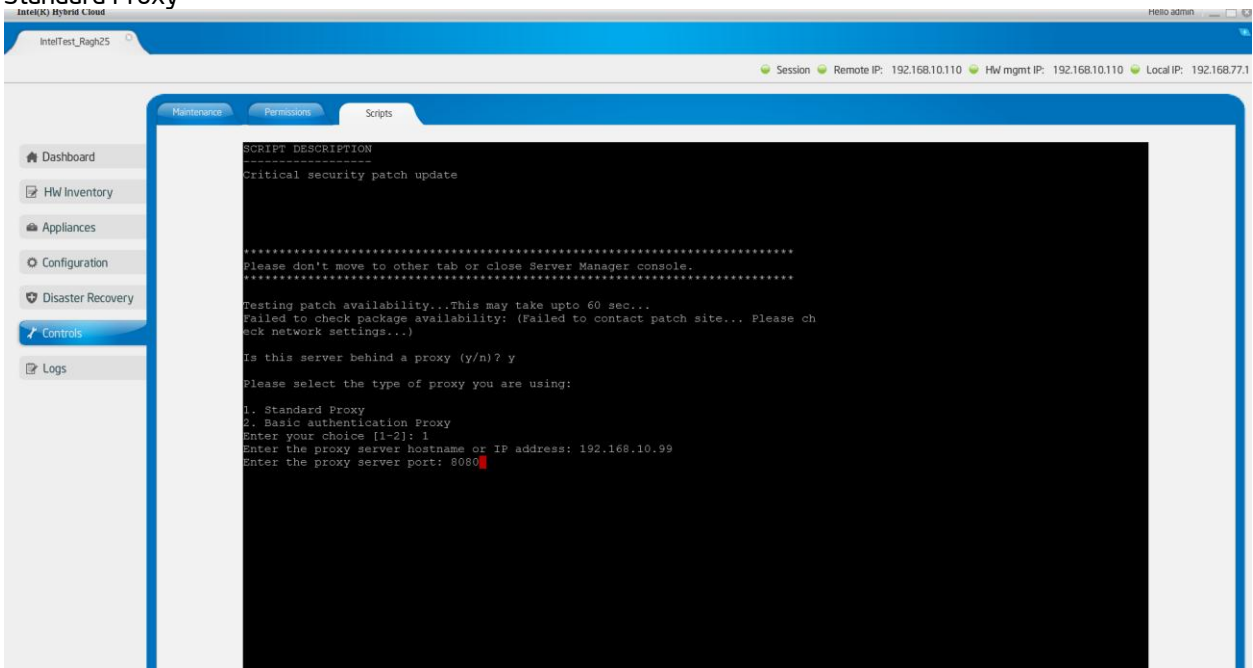There are two types of proxy versions supported.

- Standard Proxy
- Authenticated Proxy

The screen shots below show how the Script will work when there is a proxy and the IHC system is connected to the proxy
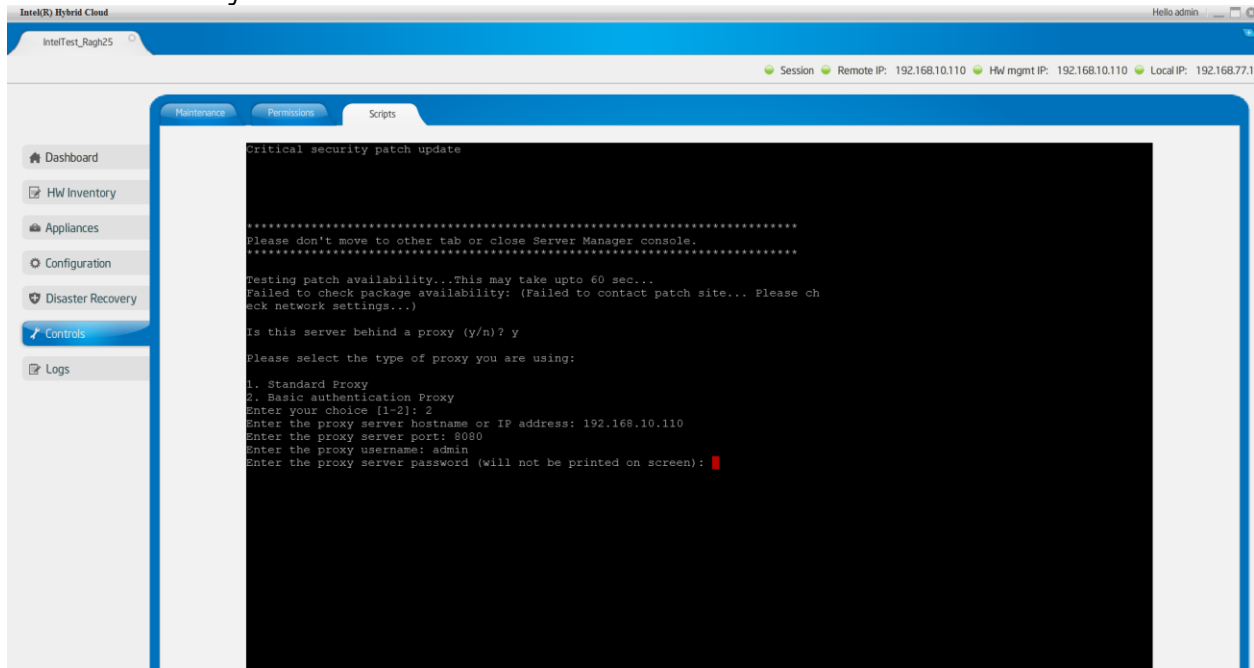
Running the script....

SCRIPT DESCRIPTION

Critical security patch update

****
Please don't move to other tab or close Server Manager console.
****

Testing patch availability...This may take upto 60 sec...
Failed to check package availability: (Failed to contact patch site... Please ch
eck network settings...)

Is this server behind a proxy (y/n)? y

Please select the type of proxy you are using:

1. Standard Proxy
2. Basic authentication Proxy
Enter your choice [1-2]:

Standard Proxy

SCRIPT DESCRIPTION

Critical security patch update

****
Please don't move to other tab or close Server Manager console.
****

Testing patch availability...This may take upto 60 sec...
Failed to check package availability: (Failed to contact patch site... Please ch
eck network settings...)

Is this server behind a proxy (y/n)? y

Please select the type of proxy you are using:

1. Standard Proxy
2. Basic authentication Proxy
Enter your choice [1-2]: 1
Enter the proxy server hostname or IP address: 192.168.10.99
Enter the proxy server port: 8080

Authenticated Proxy

Please contact Intel Customer Support if you have an issue installing the security update or need further assistance.
http://www.intel.com/support/motherboards/server/hybrid/sb/CS-032313.htm

Intel Hybrid Cloud Organization
Intel Corporation