Remediating UDP Source Port Pass Firewall Vulnerability on ESXi servers

ESXi uses a stateless firewall. Consequently, it has a rule to allow incoming DNS traffic (UDP) through source port 53. The easiest way to fix this vulnerability is to restrict the access on this port to the local DNS server IP addresses.

You can restrict access either using the vSphere Web Client or VMware PowerCLI. Instructions for each method are below.

Using the vSphere Web Client

1. Access the vSphere web client.
2. Login into vCenter and navigate to the Hosts and Cluster view.
3. In the left hand navigation panel, click on the host you would like to update.
4. Click the Configure tab and select Security Profile.
5. Scroll up and click on Edit to edit the firewall.
6. In the popup window, make the following changes.
   - Select DNS Client
   - If it is selected, deselect Allow connections from any IP address
   - Enter a comma separated list of DNS server IP addresses
7. Click **Ok**.

**Using VMware PowerCLI**
You can use the following PowerCLI commands to automate the updating of all of your ESXi servers. You will need to add a few additional lines of code to fetch ESXi hostnames and such.

```
$ESXfw = (get-esxcli -vmhost <ESXiHOST>).network.firewall
$ESXfw.ruleset.set($false,$true,"dns")
$ESXfw.ruleset.allowedip.add("171.64.1.234","dns")
$ESXfw.ruleset.allowedip.add("171.67.1.234","dns")
```