Dear Cisco Customer,

Cisco engineering has identified the following software issues with the release that you have selected that may affect your use of this software. The software is no longer available for download. Please review the Software Deferral notice here to determine if the issues apply to your environment.

For more comprehensive information about what is included in this software, refer to the Cisco software Release Notes, available from the Product Selector tool. From this page, select the product you are interested in. Release Notes are under "General Information" on the product page.

| Affected Software and Replacement Solution for *CSCvp90129* | | |
|---|---|---|
| **Software Type** | **Software Affected** | **Software Solution** |
| Cisco HyperFlex Data Platform Software | **Version:** HX Data Platform 3.5(2c) in a Stretched Cluster configuration<br><br>**Affected Images:** *Cisco-HX-Data-Platform-Installer-v3.5.2c-31725-esx.ova* | **Version:** 3.5(2g)<br><br><br>**Replacement Images:** *Cisco-HX-Data-Platform-Installer-v3.5.2g-32110-esx.ova* |

**Reason for Advisory:**
This software deferral addresses one software issue.

**CSCvp90129**:
Stretched Cluster nodes that experience failures may become unavailable

**Affected Platforms:**
Cisco HyperFlex Systems running the software version HyperFlex HX Data Platform 3.5(2c) in a Stretched Cluster configuration with the following hardware platforms

- HX220C-M5SX
- HX240C-M5SX
- HXAF220C-M5SX
- HXAF240C-M5SX
- HX240C-M5L

**Symptom**:
On Stretched Clusters, if the cluster experiences a node or disk failure, adds additional nodes or disks, or a maintenance window that results in rebalance, some nodes in the cluster may become unavailable.

**Conditions:**
To be susceptible to CSCvp90129, the HyperFlex cluster must be running an M5 hardware platform as listed above and configured in a Stretched Cluster configuration. HyperFlex on Hyper-V and standard HX clusters are not affected by this defect.

**Workaround:**
If a Stretched Cluster configuration has been upgraded to the affected release - please contact Cisco support.