



Software Advisory Notice

Cisco has identified the following software issue with the release that you have selected that may affect your use of this software. Review the Software Advisory notice here to determine if the issue applies to your environment. You may proceed to download this software if you have no concerns with the issue described.

For more comprehensive information about what is included in this software, refer to the documentation at the following site:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Affected Software and Replacement Solution for CSCv04251		
Software Type	Affected Software Versions	Fixed Software Versions
Cisco NX-OS for the Cisco Nexus 9000 series switches in the ACI mode	14.2(2e), 14.2(2f), 14.2(2g), 14.2(3j), 14.2(3l), 14.2(3n), 14.2(3q), 14.2(4i), 14.2(4k), 14.2(4o), 15.0(1k), 15.0(1l), 15.0(2e)	14.2(4p) and later 14.2 releases 15.0(2h) and later releases

Issue Description

Known defect CSCv04251 causes a policy upgrade to fail on the Cisco N9K-C9316D-GX and N9K-C93600CD-GX platforms that have the hw_changes_bit programmed as "0x03." To see the hw_changes_bit value, use the following CLI commands:

```
# vsh  
  
# show sprom cpu-info  
  
HW Changes Bits : 0x3
```

This issue occurs only when you attempt to upgrade Cisco N9K-C9316D-GX and N9K-C93600CD-GX switches from an affected software version to a subsequent release. Outside of the upgrade process, Cisco N9K-C9316D-GX and N9K-C93600CD-GX switches running the affected software versions will operate under normal conditions.

Workaround

If you want to upgrade the software in your switches, use the following workaround to avoid the issue:

1. Upgrade the Cisco APICs and other devices in the fabric, except for the Cisco N9K-C9316D-GX and N9K-C93600CD-GX switches that are running one of the affected software versions.
2. Contact Cisco TAC and request for the TAC personnel to apply the workaround patch manually on the Cisco N9K-C9316D-GX and N9K-C93600CD-GX switches that are running one of the affected software versions.

3. After the workaround patch is applied to the affected Cisco N9K-C9316D-GX and N9K-C93600CD-GX switches, you can perform the normal policy-based upgrade on these switches.