*** CAUTION - PI 3.5 Update 03 ***

1. **PI 3.5 Update 03 should only be installed on PI 3.5 (PI 3.5 Update 01, or PI 3.5 Update 02)**
2. **If you haven't installed PI 3.5 Update 01 yet, then this is a *** critical mandatory update *** - it should only be installed on a PI 3.5 server. Also, if you plan to restore a backup of a prior PI 3.x release on a freshly installed PI 3.5 server, then install PI 3.5 Update 03 prior to initiating a restore of that backup.**
3. **If you are using a VM environment for running PI, please ensure that the disk is using thick provisioning, otherwise patch install process may take a very long time to complete.**
4. If you are unable to download this package directly from cisco.com through **Administration** -> **Software Updates** page, then please download this update to your local machine and manually upload and install it through PI's Software Updates page.

Introduction

This UBF includes defect fixes. This mandatory update should **only** be installed on a Cisco Prime Infrastructure 3.5 server. This update addresses following defects:

Security Vulnerability Fixes:

Defect	Headline
CSCvj92813	Cisco Prime Network Control System Stored Cross-Site Scripting vulnerability
CSCvo28671	Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution
CSCvo28666	Cisco Prime Infrastructure and Evolved Programmable Network Manager Path Traversal vulnerability
CSCvo28677	Cisco Prime Infrastructure and Evolved Programmable Network Manager Path Traversal vulnerability
CSCvo28680	Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution
CSCvo28684	Cisco Prime Infrastructure and Evolved Programmable Network Manager Path Traversal vulnerability
CSCvo23576	Cisco Prime Infrastructure and Evolved Programmable Network Manager SQL Injection vulnerability
CSCvo22842	Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution
CSCvo28734	Cisco Prime Infrastructure and Evolved Programmable Network Manager SQL Injection vulnerabilities

Please refer to Cisco's PSIRT site for more detail on all the **Security Vulnerability** issues.

Resolved in PI 3.5 Update 03

Defect	Headline
CSCvo59546	Need to correct the AP Groups max limit for a few WLC platforms
CSCvo32128	AP configuration changes fail when associated controllers are running IOS XE 3.6.x or 3.7.x
CSCvp40274	PDF Generation Fails for Unique Clients Report
CSCvo50884	Save and Export with pdf is failing for fault events and syslog report
CSCvo48503	Schedule update for existing reports is not reflected in GUI
CSCvo95226	'No Metrics available for this Interface.' warning message in Performance Graphs
CSCvp57581	Unable to search templates of lightweight access points

Resolved in PI 3.5 Update 02

Defect	Headline
CSCvn71019	Devices are not visible in the Network Devices tab under All Devices
CSCvn85425	In PI, attempt to migrate groups to Cisco DNA Center 1.2.8 fails
CSCvn74996	PI co-existence servers filed input - Getting XSS Alert
CSCvo15468	Unable to deploy WLAN Template with "Flex Local Auth" enabled
CSCvn63394	ClientApModeEnum has to support more values related to additional AP modes
CSCvo33279	"End User Experience" dashlet does not load data when client filter contains a backslash character
CSCvn85601	In PI, non-root users can't run "capture copy" job or the view jobs when not mapped to ROOT-DOMAIN
CSCvm93515	Netflow data shown in NAM and PI does not match
CSCvo45612	Old AP name is visible in GUI after it is changed through the Prime Infrastructure API
CSCvo00101	User created application does not show in the All Applications table of Japanese GUI
CSCvn79593	Unable to edit some non-root virtual domain maps
CSCvo47361	Post PI upgrade, one cannot delete the CMX Import map file
CSCvo09578	Prime Infrastructure lists incorrect model name in device hardware EOX report
CSCvo25853	Incorrect message shown in stage 8 when one restores a 32X (or 34X) backup on PI 3. 5 Update 01
CSCvo50802	Gen 3 server displays Serial identifier as 'UNSUPPORTED'
CSCvo19314	Copy and Replace APs functionality is broken
CSCvn67011	Poller_PostLradIfChannelStatsRecord Unknown Exception log in error level floods the syslog server
CSCvo46980	In PI 3.5 the lradtemplate does not load in the UI
CSCvo47377	PI-DNAC migration hangs with a SSH authentication failure

CSCvo46693	With 16.10.1e, AP cleared Alarms are not reflected on maps, it still shows a yellow icon on the map
CSCvo26017	With Unified APs, PI shows a "Permission Denied" error when one clicks on the Configuration tab
CSCvo20966	PI 3.5 shows a mismatch in clients' count when they roam across WNCs
CSCvo56692	Top N Memory Utilization dashlet does not filter devices when selecting a site.
CSCvo32288	In PI 3.5, the ReachableAp5MinuteAggregator table is missing

Resolved in PI 3.5 Update 01

Defect	Headline
CSCvn61377	Client count report is throwing an error when generated with the "Report By criteria"
CSCvo26071	In PI's Operation Center (OPC), "Avg API Response" cross launch reports an error
CSCvm54241	Advanced Search via "Application Search" is restricting access
CSCvo27397	Clients and Users page showing "No data found"
CSCvn49224	Client count threshold in Health Rules
CSCvn47334	In PI, unable to login as webroot user after migration
CSCvn92947	Inaccurate client count on maps AP info view for 802.11a/n/ac radio
CSCvn66302	Prime Infrastructure doesn't see the second interface, eth1
CSCvn77526	Prime Infrastructure fails to generate map tiles in AP planning mode
CSCvi72508	In HA, AESUID_SEQUENCE mismatch between Primary and Secondary can cause side effects
CSCvo22809	AP and CAPWAP uptimes are showing wrong data
CSCvn99371	Device parameters are missing after upgrading to PI 3.5
CSCvo02416	Problem with Previous Calendar Day Reports only reporting 23 hrs data
CSCvn79940	On-Demand Run Action issue on Reports

There are no other new features included in this update.

System Requirements

For more information on server and web client requirements, see the System Requirements section of the *Cisco Prime Infrastructure 3.3 Quick Start Guide*.

Installation Guidelines

The following sections explain how to install the patch.

Before You Begin Installing the Patch

Caution: Once you install this patch, you cannot un-install or remove it. If this is VM based environment, then if possible, take a VM Snapshot before applying this patch. It is recommended that you always take a backup before attempting to install an update.

Because the patch is not removable, it is important to have a way to revert your system to the original version in case hardware or software problems cause the patch installation to fail.

To ensure you can do this, take a backup of your system before downloading and installing this UBF patch.

Cautionary Note: ***Do not*** restore a PI 3.5 backup on a PI 3.5 server! Take a backup only after you have installed PI 3.5 Update 03. Also, if needed, restore a prior release backup only on a PI 3.5 Update 03 (or higher) setup.

To revert back to Prime Infrastructure 3.5 installation (with PI 3.1.x, PI 3.2.x, PI 3.3.x, PI 3.4.x, or a PI 3.5 backup), follow these steps:

1. Reinstall Prime Infrastructure 3.5 from an OVA or ISO distribution
2. Install PI 3.5 maintenance release
3. Install this update (PI 3.5 Update 03)
4. If you have a prior PI 3.1.x, PI 3.2.x, PI 3.3.x, PI 3.4.x, or PI 3.5 backup
   - Restore this backup

If you are installing the patch as part of a High Availability (HA) implementation, you will want to ensure that the network links between the two servers provide maximum bandwidth and low latency throughout the patch install. For more information, see Troubleshooting Patch Installs in HA Implementations.

Note: Some of the links refer to prior releases because the instructions included in those documents are still valid.

Installing the PI_3_5_Update_03-1.0.9.ubf patch

Make sure you have completed the recommended preparation steps given in Before You Begin Installing the Patch.

If you are currently using Prime Infrastructure without enabling High Availability, follow the steps

below to install the patch.

Step 1 **Download** the patch file (**PI_3_5_Update_03-1.0.9.ubf**), and save the file locally.

Step 2 Log in to the Prime Infrastructure server using an ID with administrator privileges and choose **Administration > Software Update**.

Step 3 Click **Upload Update File** and browse to the location where you saved the patch file. Click **OK** to upload the file.

Step 4 When the upload is complete:

a. On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.

b. Select the patch file and click **Install** .

c. You will see a popup message indicating when the installation is complete. You should also see a listing for the patch in the "Updates" table, with a "Yes" opposite the patch under the "Installed" column, and a "Yes" under the "Pending Restart" column.

Step 6 As a final step of the install process, the server restart will be triggered automatically (**Note**: **you should not** manually execute ncs stop followed by ncs start)

Step 7 Verify that the patch is installed by logging into the server and choosing **Administration > Software Update** . You should see a listing for the patch in the "Updates" table, with a "Yes" opposite the patch under the "Installed" column, and a "No" under the "Pending Restart" column.

Installing the PI_3_5_Update_03-1.0.9.ubf With High Availability

Make sure you have completed the recommended preparation steps given in Before You Begin Installing the Patch.

Remove HA Via the GUI (as outlined Cisco Prime Infrastructure 3.4 Administrator Guide). Continue the patching once HA is removed completely. For more details, see the How to Patch New HA Servers section in the Cisco Prime Infrastructure 3.4 Administrator Guide.

Patching of the primary and secondary server takes approximately one hour. During that period, both servers will be down. If you have trouble at any point, see Troubleshooting Patch Installs in HA Implementations.