Release Notes for Cisco Edge 340 Series, Release 1.2 Patch 20

First Published: September 19, 2016

These release notes include important information about Cisco Edge 340 Series Software release 1.2 patch 20 and the limitations, restrictions, and caveats, if any, that apply to this release.

Contents

System Requirements

Hardware Supported

Table 1 Cisco Edge 340 Series Supported Hardware

Model No.	Description
CS-E340W	Cisco Edge 340 Series (Wireless)
CS-E340	Cisco Edge 340 Series (Non-wireless)

Software Images

Filename	Description
ce340-1.2-patch-0.21.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 21
ce340-1.2-patch-0.20.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 20
ce340-1.2-patch-0.19.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 19
ce340-1.2-patch-0.14.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 14
ce340-1.2-patch-0.12.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 12
ce340-1.2-patch-0.11.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 11
ce340-1.2-patch-0.9.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 9
ce340-1.2-patch-0.6.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 6
ce340-1.2-patch-0.5.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 5
ce340-1.2-patch-0.4.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 4
ce340-1.2-patch-0.2.tar.gz	Cisco Edge 340 Series Release 1.2 OS Patch 2
Cisco-Edge-1.2-i386-DVD.bin	Cisco Edge 340 Series Release 1.2 OS

Chrome 31 Patch

This is a generic patch for CE340 release 1.2.0.x to update the chrome 31 version.

Note The Chrome patch should be applied after the OS patch installation.
For example, if you are going to upgrade from release 1.2 to release 1.2.0.6, follow this order: 1.2 -> 1.2.0.6 -> CE340_Chrome-31_patch-0.6.tar.gz.

Follow these steps to install the Chrome 31 patch:

Step 1 Log in to the Cisco Edge 340 Series system as root with terminal through SSH or Desktop.

Step 2 Copy or download the patch file to the Cisco Edge 340 Series filesystem.

Step 3 Follow these steps to install the patch:

a. Use the following command to uncompress the patch, for example, to the `/tmp` folder:

```
# tar xvzf $folder/ce340_Chrome-31_patch.tar.gz -C /tmp/
```

b. Go to the target folder where you uncompressed the patch and run the `install.sh` file to install the patch management tool:

```
# cd /tmp/ce340_Chrome-31_patch
# /bin/sh install.sh --force
```

Step 4 After the patch is installed successfully, run the following command to check the version:

```
# cpg_patch_ctl --get version
```

You can get more information by using the following command:

```
# cpg_patch_ctl --help
```

Step 5 Execute the **reboot** command manually if necessary.

Step 6 Verify the functions implemented by this patch after reboot.

Note The patch cannot be uninstalled or rolled back.

Upgrading to a New Software Release

The Cisco Edge 340 series supports the following installation and upgrade methods:

- USB Mode Installation and Upgrade, page 3
- Remote Upgrade From the Web GUI, page 5
- BIOS Upgrade, page 6
- Patch Installation, page 6

USB Mode Installation and Upgrade

The Cisco Edge 340 Series software releases a self-extract installer. The file name is Cisco-Edge-*version*-i386-DVD.bin. It is an executive file that helps you to perform the installation automatically. When you execute the self-extract installer, the installation-related files are extracted to the hard drive of the Cisco Edge 340 Series, and a livecd is created in the internal USB. The system then boots from the internal USB (also known as the factory mode) and performs the installation automatically.

If the internal USB has already been created as a livecd, you can press the factory mode pinhole on the front panel of the Cisco Edge 340 Series to enter the factory mode and perform the installation procedure automatically.

Note Usually, the internal USB is created as a livecd in the factory. Executing the self-extract installer will overwrite the original livecd and create a new one.

Prerequisites

Before you execute the self-extractor installer, perform the following steps to make sure that the installation will be successful.

Step 1 Locate your target self-extract installer (Cisco-Edge-xxx-i386-DVD.bin).

Step 2 Make sure that the livecd-tools has been installed using the following command:

```
rpm -q livecd-tools
```

Step 3 Make sure there is at least 1.5G free space on HOME or ROOT partition. If you execute the self-extractor installer without enough space on the partition, you will see the either of the following message displayed: *No enough disk free space* or *Failed to extract ISO!*

- Use the following command to check the available space on the HOME partition:

  ```
  df -h /home
  ```

- Use the following command to check the available space on the ROOT partition:

  ```
  df -h /
  ```

Step 4 If you want to use an external USB as the target USB, make sure the first partition of the USB has at least 1.5G free space. The ext4 format is recommended, and ext3/fat32 format is also supported.

Step 5 Make sure the self-extract-installer (Cisco-Edge-xxx-i386-DVD.bin) has the executable attribute. Set the attribute with the following command:

```
chmod a+x /path/to/ Cisco-Edge-xxx-i386-DVD.bin
```

Step 6 Make sure no other installation or upgrade process is ongoing.

Note If another installation or upgrade process is ongoing, and you execute the self-extractor installer, you will see the following message displayed: *an install process is ongoing*. You can wait until the ongoing upgrade process is finished, or you can reboot the system, and then execute the self-extractor installer again.

Note When you select the internal USB as target livecd, if power failure happens during the process of command execution, the old livecd on the internal USB will be wiped. You have to rebuild a livecd disk on the internal USB.

Command Description

You can use the Cisco-Edge-*version*-i386-DVD.bin command with different parameters to implement installation or upgrade, print help, or create livecd only. In the command, *version* indicates the image version, which will be 1.2 for this release. For detailed instructions of installation and upgrade for this release, see *Cisco Edge 340 Series Software Configuration Guide, Release 1.2*.

For the installation and upgrade of the releases other than 1.2, refer to the software configuration guide of corresponding releases.

Note When you use this method to install or upgrade the system, make sure there is 1.5G free space at least.

1. To select the internal USB as a livecd disk and boot into factory mode to finish the installation automatically, use the following command:

   ```
   Cisco-Edge-1.x-i386-DVD.bin
   ```

2. To print help and then exit, use the following command:

   ```
   Cisco-Edge-1.x-i386-DVD.bin --help|-h
   ```

3. To create livecd only, without entering factory mode nor executing the system installation program, use the following command:

   ```
   Cisco-Edge-1.x-i386-DVD.bin -t|--target <dev>
   ```

   <dev> is the full path of the target u-disk into which the livecd will be burned, for example, /dev/sdb1.

4. To wipe the home partition before the system is installed, use the following command:

```
Cisco-Edge-1.x-i386-DVD.bin -w|--wipe
```

Note When the home partition is wiped, user data will be lost.

Installation With External USB

Follow these steps to upgrade your Cisco Edge 340 Series to software release 1.2 with an external USB:

Step 1 Get a Fedora PC.

Step 2 Attach a USB flash drive to the PC.

Step 3 Download Cisco-Edge-1.2-i386-DVD.bin to the PC.

Step 4 Execute the following commands in shell:

```
su -c "chmod +x Cisco-Edge-1.2-i386-DVD.bin"
su -c "./Cisco-Edge-1.2-i386-DVD.bin -t /dev/sdb1"
```

Replace sdb1 in the above command with your own USB and wait until the command is completed.

Step 5 Detach the USB flash drive from the PC and attach it to your Cisco Edge 340 Series device.

Step 6 Boot your Cisco Edge 340 Series from the USB.

Step 7 Wait for the installation to complete and then reboot the device.

Installation With Internal USB of the Cisco Edge 340

Follow these steps to upgrade your Cisco Edge 340 Series to software release 1.2 with the internal USB:

Step 1 Download Cisco-Edge-1.2-i386-DVD.bin to the SSD of your Cisco Edge 340 Series device.

Step 2 Execute the following commands in shell:

```
su -c "chmod +x Cisco-Edge-1.2-i386-DVD.bin"
su -c "./Cisco-Edge-1.2-i386-DVD.bin"
```

Step 3 Wait for the installation to complete and then reboot the device.

Remote Upgrade From the Web GUI

You can perform a remote upgrade for the Cisco Edge 340 Series using the web GUI if you have the address to download the self-extract installer. When you choose to perform the remote upgrade, the system will automatically download the self-extract-installer from the URL that you provide and execute the self-extract-installer to finish the installation.

BIOS Upgrade

BIOS upgrade can only be performed by manually installing the package and executing the commands in the Linux environment. BIOS is a critical part of the system, and there is no software recovery method if it crashes. To ensure successful BIOS upgrade, make sure that the external power supply is always connected, and do *not* perform any power cycle action during the upgrade process.

Patch Installation

Before installing a new software patch, you must already have the corresponding release image and all the patches released before this patch installed on your system.

Follow this procedure to install a new software patch:

Step 1 Log in to the Cisco Edge 340 Series system as root with terminal through SSH or Desktop.

Step 2 Copy or download the patch file to the Cisco Edge 340 Series filesystem.

Step 3 Follow these steps to install the patch:

a. Use the following command to uncompress the patch, for example, to the `/tmp` folder:

```
# tar xvzf $folder/ce340-1.2-patch-0.x.tar.gz -C /tmp/
```

b. Go to the target folder where you uncompressed the patch and run the `install.sh` file to install the patch management tool:

```
# cd /tmp/ce340-1.2-patch-0.x
# /bin/sh install.sh --force
```

Step 4 If the cpg_patch_ctl tool is already installed, use it to install the patch by using the following command:

```
# cpg_patch_ctl -f -i $folder/ce340-1.2-patch-0.x.tar.gz
```

Note You cannot use the cpg_patch_ctl tool to install release 1.2 patch 12 and 14. It is a known issue. For details, see CSCuw35253 in the "Known Issues" section on page 13.

If the patch is installed successfully, the following message will be displayed:

```
'INFO: Patch installed successfully.'
```

Otherwise, an error message will be displayed:

```
'ERROR: <ERROR Message>'
```

If the patch is already installed, the installation will be aborted and the following warning will be displayed:

```
'WARNING: Patch already installed. Abort.'
'WARNING: If you want to re-install, please add "--force" option to "cpg_patch_ctl" tool'
```

If you want to reinstall the patch, use the **`/bin/sh/install.sh --force`** command to install the patch in force mode, or add the **`--force`** option when using the **`cpg_patch_ctl`** command.

Step 5 To check persistency, you can run the preinstall script, **`ce340-1.2-patch-0.x/system/pre-install.sh`** before installing the patch, and run the post-install script **`ce340-1.2-patch-0.x/system/post-install.sh`** after installing the patch file RPMs.

Note Make sure the pre-install and post-install scripts can be run for multiple times due to "--force" option.

Step 6 After the patch is installed successfully, run the following command to check the version:

```
# cpg_patch_ctl --get version
```

You can get more information by using the following command:

```
# cpg_patch_ctl --help
```

Step 7 Execute the **reboot** command manually if necessary.

Step 8 Verify the functions implemented by this patch after reboot.

Note The patch cannot be uninstalled or rolled back.

Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the *Cisco Edge 340 Series Software Configuration Guide*.

New and Changed Information

This section contains new and changed information for this release.

New Software Features in Release 1.2

Release 1.2 introduces the following new software features:

- SIP video call plug-in enhancement
  - Supports the call-hold function.
  - Supports the call-mute function for audio and video respectively.
  - Supports to accept call transfer requests from CUCM.
  - Supports RFC2833 DTMF.
  - Supports to monitor statistics during a phone call.
  - Supports to enable or disable the preview function.
  - Supports to configure resolution of both local video and output video.
  - Supports to negotiate resolution through SIP/SDP.
  - Supports to configure download and upload bandwidth.
  - Enables bit-rate adaptation according to current resolution and bandwidth.
  - Improved echo cancellation by making parameters adjustable.

  - Updated compatible collaboration endpoints list of collaboration devices.
- 802.1x authentication
  - Supports 802.1x authentication client.
  - Supports to enable or disable the 802.1x authentication function on Web GUI.
  - Supports to configure username and password on Web GUI.
  - Supports three authentication methods: EAP-TLS, PEAP, and EAP-FAST.
- Supports SNMP v1, v2.
- SNMP trap—Supports to detect the changes on CPU usage, CPU temperature, memory usage, storage usage, interface status changes, and syslog updates. Supports to configure the threshold on Web GUI. Supports to enable or disable the SNMP trap function on Web GUI (disabled by default).
- Radius authentication—Supports to enable or disable Radius authentication on Web GUI. Supports to configure Radius server on Web GUI. Supports the role of 'root' only.
- PoE enhancement—Supports to configure power requests on Web GUI via CDP.
- Enabling or disabling USB port—Supports to enable or disable a specific USB port on Web GUI.
- Enabling or disabling IR—Supports to enable or disable IR on Web GUI.
- Volume indicator—Supports to indicate volume status and enable or disable this indicator on Web GUI.
- Reimage via IR—Supports to pop up a window on desktop or in kiosk mode by pressing key A on the IR remote, which will later guide you to restore to the factory mode. In the factory mode, the device will be reimaged, and all user data and configurations will be wiped out. Password required to verify this reimage option is configurable on Web GUI.
- Show patch version—Supports to display the latest installed patch version on Web GUI.
- Enabling or disabling Grub message—Supports to enable or disable grub message on Web GUI.
- Import third party certifications—Supports to import third party certifications only by HTTP API.
- Network monitor enhancement—Supports to monitor VPN status on Web GUI.
- Default route—Supports to configure default route in STA mode for WiFi client on Web GUI.
- Bi-directional RS-232—Supports HTTP API of serial port communication. Supports to send a command to a TV set and wait for the response within 1 second. Fully supports all special characters whose ASCII values are smaller than 20 or larger than 127.

Note No parsing will be done on the response. Any reply that is longer than 60 will be cut off.

- Log rotation for Nginx—Supports to compact the obsolete logs automatically and delete them on the next day. This function is enabled by default.

Limitations and Restrictions

This section contains limitations and restrictions of the Cisco Edge 340 Series.

- The Cisco Edge 340 Series device supports HDMI 1.3 only.
- The supported video bit rate is up to 20 Mbps, and the supported audio bit rate is up to 512 Kbps.

- To avoid flickering of the videos that contain flash content, a one-pixel black border will be present when the Cisco Edge 340 is playing a video with flash plugin on Appspace.

Caveats

This section provides open and resolved caveats in release 1.2.

Open Caveats in Release 1.2

- CSCuj03737

  Due to Intel graphic driver issue, you may run into the following issues:

  a. During VLC playback, you may occasionally find the following issue, and the workaround is to use 30fps instead of 60fps:

  – Frame-drop and tearing occurred in the 720p60fps video with CC in 1920x1080 resolution.

  b. In extend mode, you may occasionally find the following issues, and the workaround is to reboot the system:

  – The HDMI monitor displays instability in extend mode only.

  – In the extend mode, rotating HDMI display causes error.

  – In two-channel extend mode, VLC cannot be killed after one channel is paused.

  c. When setting up display, you may occasionally find the following issues, and the workaround is to reboot the system:

  – Nothing is displayed after switching the monitor from VGA to HDMI.

  – HDMI monitor displays black screen occasionally when hot-plugin.

- CSCun47114

  VLC streaming play back related issues.

  – Network environment may significantly impact the quality of video stream.

  – Big mosaic on MPEG2 video stream.

  – VLC media player cannot play HTTP network stream (YouTube).

  There is no workaround.

- CSCur01740

  Sometimes the CPU usage of Xorg server will be high and close to 100% after some specific operations like hot-plug, or rarely during video transaction, which will cause system to hang and no response to other programs.

  The workaround is to reboot.

- CSCun85503

  Image upgrade failed when uploading spent more than 5 minutes, while downloading works well.

  The workaround is to make sure the image uploading takes less than 5 minutes or choose another upgrade method.

- CSCui73253

  VLC plugin cannot play smoothly with different codec videos in one browser.

  The workaround is to play videos of the same codec.

Resolved Caveats in Release 1.2 Patch 21

- CSCuz44338

  Evaluation of ce340 for NTP_April_2016.

- CSCuz52515

  Evaluation of ce340 for OpenSSL May 2016.

Resolved Caveats in Release 1.2 Patch 20

- CSCva19955

  Adobe flash vulnerability.

  This patch will address below Adobe vulnerability issue. The updated version of adobe flash will be 11.2.202.626.

  https://helpx.adobe.com/security/products/flash-player/apsb16-15.html

  After applying this upgrade, the customer will cease to get the hardware acceleration from flash player. It is recommended to use only after thorough understanding of the impact.

Resolved Caveats in Release 1.2 Patch 19

- CSCur42263

  Edge 340 IP/GW settings cannot be saved or changed via mgtcmd.

- CSCuz04213

  DHCP Kernel Panic issues.

- CSCuy07443

  Evaluation of ce340 for OpenSSL January 2016-PSIRT.

- CSCuy35299

  Evaluation of ce340 for glibc_feb_2016.

- CSCux95195

  Evaluation of ce340 for NTP_January_2016.

- CSCuz30648

  Wireless Hidden SSID Fix.

- CSCuy54700

  Evaluation of ce340 for OpenSSL March 2016.

Resolved Caveats in Release 1.2 Patch 14

- CSCuv11236
  CE340 SIP HA Feature.

Resolved Caveats in Release 1.2 Patch 12

- CSCuu13834
  Certificate auto enroll or renewal should be supported (SCEP).

Resolved Caveats in Release 1.2 Patch 11

- CSCuu82505
  Evaluation of CE340 for OpenSSL June 2015.

Resolved Caveats in Release 1.2 Patch 9

- CSCut84826
  Failed to update contact with REST API.
- CSCut62989
  SNMPWALK does not return expected results.
- CSCut46083
  MARCH 2015 OpenSSL Vulnerabilities.
- CSCuu43968
  Cisco Edge 340 File Disclosure Vulnerability.

Resolved Caveats in Release 1.2 Patch 6

- CSCus70820
  Proxy with authentication always prompted for authentication.

Resolved Caveats in Release 1.2 Patch 5

- CSCut12139
  Hostname changed by DHCP server when no DHCP option 12 request sent.

Resolved Caveats in Release 1.2 Patch 4

- CSCut08022
  Edge 340 does not register with Wireless hidden SSID.

Resolved Caveats in Release 1.2 Patch 2

- CSCus21146

  Edge 340 does not support interlace in the MPEG2 software decoding mode.
- CSCus70853

  VLC plugin takes more than 10s for HLS stream switch.
- CSCus69652

  Evaluation of glibc GHOST vulnerability - CVE-2015-0235.

Resolved Caveats in Release 1.2

- CSCun70198

  Network manager crashed occasionally after switching the WiFi mode.
- CSCun80404

  Connection will be lost in high-density Extended Service Set (ESS) network.
- CSCun96138

  CE340 cannot reconnect to the ASUS AP RT-N56U after disconnected.
- CSCuo10636

  DNS server got from VPN still presents when connection is unestablished.
- CSCun23000

  PPTP automatic reconnecting does not work in AP mode.
- CSCup41424

  When there is no space left in the root partition on the Cisco Edge 340, it will not be able to log in or not be able to run some applications.
- CSCur05619

  Edge 340 Digital Media Player eval for the security issue of CVE-2014-6271 and CVE-2014-7169.
- CSCur30222

  TLS/SSL server supports SSL version 3 to solve the security issue of POODLE/CVE-2014-3566.
- CSCur43343

  VLC plugin in Chrome will crash when transiting from one video to another.
- CSCuq53899

  User space will be fully occupied by Nginx logs.
- CSCun99096

  Autologin may not work if registering a new CE340, which is not compatible with release 1.0.5.
- CSCun67800

  Kernel error being printed continuously after player or plugin is closed abnormally, which will cause the system hanging for a while.
- CSCup59010

  HLS stream pauses and delays.

- CSCup87707

  CE340 GUI will not accept IP with 255 in the third octet for a DNS server.

- CSCuo77756

  The mouse is not moving smoothly after being plugged out and plugged in again.

- CSCuo84574

  The login page is in Chinese after the language is set to Spanish.

- CSCuo34203

  Cannot get resolution list on Web GUI with Cisco 42’ LCD.

- CSCuo21086

  The coordinates are not correct on the test web page when the touch mode is set to multi-touch.

- CSCup48500

  There is black background flickering between video transitions in VLC plugin.

- CSCuo23755

  OpenSSL heartbeat issue. A missing bound check was found in the way OpenSSL handled TLS heartbeat extension packets.

- CSCup24248

  Multiple vulnerabilities in OpenSSL - June 2014.

  - CVE-2010-5298—SSL_MODE_RELEASE_BUFFERS session injection or denial of service.
  - CVE-2014-0076—Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack."
  - CVE-2014-0195—DTLS invalid fragment vulnerability.
  - CVE-2014-0198—SSL_MODE_RELEASE_BUFFERS NULL pointer dereference.
  - CVE-2014-0221—DTLS recursion flaw.
  - CVE-2014-0224—SSL/TLS MITM vulnerability.
  - CVE-2014-3470—Anonymous ECDH denial of service.
  - CVE-2014-4877—Wget FTP Symlink arbitrary filesystem access.

Known Issues

This sections provides the closed defects and known issues for the Cisco Edge 340 Series, release 1.2.

- CSCuo23986

  The rescue mode cannot be displayed via HDMI output.

  This is an Intel issue that cannot be fixed. The workaround is to use VGA to enter rescue mode.

- CSCuo26650

  Playing 1080P-H264-MP4 video in portrait mode joggled.

  This is a TPI issue that cannot be fixed. The workaround is to use VLC plugin.

- CSCuo29278

  Edge 340 screen froze at MPEG2 video stream in WiFi station mode.

This is an Intel issue that cannot be fixed. The workaround is not to play RTP streaming in MPEG2 codec in WiFi station mode.

- CSCuj49538

  HTTP stream playback is not smooth and likely to block in two channels mode.

  This is a VLC issue that cannot be fixed. The workaround is not to play two HTTP streams in VLC or VLC plugin.

- CSCuo35575

  Dual display in the extend mode is not supported.

  This is a VLC issue that cannot be fixed. The workaround is not to play two videos at the same time in the extend mode.

- CSCuw35253

  Not able to install patch on CE340 with "cpg_patch_ctl" tool.

- CSCuw59714

  Not able to login after restting a password with the special character “#”.

  The workaround is to reset a password without the “#” symbol.

Related Documentation

These documents provide detailed information about the Cisco Edge 340 Series device and are available at:

http://www.cisco.com/go/cisco_edge_340

http://www.cisco.com/go/cisco_edge_340_s

- *Cisco Edge 340 Series Software Configuration Guide*
- *Cisco Edge 340 Series Installation Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.