Release Notes for the Cisco 220 Series Smart Plus Switches Firmware Version 1.0.1.1

July 2016

These release notes describe the resolved and known issues in the Cisco 220 Series Smart Plus Switches firmware version 1.0.1.1.

Caveats for Version 1.0.1.1

These release notes describe the caveats for the following products:

Model	Description	Ports
SF220-24	24-Port 10/100 Smart Plus Switch	fa1-fa24, g1-g2
SF220-24P	24-Port 10/100 PoE Smart Plus Switch	fa1-fa24, g1-g2
SF220-48	48-Port 10/100 Smart Plus Switch	fa1-fa48, g1-g2
SF220-48P	48-Port 10/100 PoE Smart Plus Switch	fa1-fa48, g1-g2
SG220-26	26-Port Gigabit Smart Plus Switch	g1-g26
SG220-26P	26-Port Gigabit PoE Smart Plus Switch	g1-g26
SG220-50	50-Port Gigabit Smart Plus Switch	g1-g50
SG220-50P	50-Port Gigabit PoE Smart Plus Switch	g1-g50
SG220-28	28-Port Gigabit Smart Plus Switch	g1-g28
SG220-28MP	28-Port Gigabit PoE Smart Plus Switch	g1-g28
SG220-52	52-Port Gigabit Smart Plus Switch	g1-g52

These caveats apply to:

- Firmware version: 1.0.1.1
- Bootloader version for 24-port switches: u-boot-Sx220-24-1.0.0.6.bin
- Bootloader version for 48-port switches: u-boot-Sx220-48-1.0.0.6.bin

TIP As with any firmware release, please read these release notes before upgrading the firmware. We also recommend that you back up your configuration before any firmware upgrade.

For detailed information about upgrading the firmware, see the "**Upgrading the Firmware Image**" section in the administration guide for this release.

Changes

- Change OpenSSL to 1.0.2.h
- Remove Support of SSLv2/v3 & only allow TLSv1.2 for HTTPS Connection
- Removed some SSH algorithms.
- Thermal Alarm Threshold setting update.

Resolved Issues

The following table lists the resolved issues in firmware version 1.0.1.1:

Ref Number	Description
CSCuz76238	Web Interface Denial of Service Vulnerability.
CSCuz76216	Hidden Hard Coded SNMP Community String can be used to View and Modify SNMP MIB Object
CSCuz76232	Web Interface XSS Vulnerability
CSCuz76230	Web Interface CSRF Vulnerability

Ref Number	Description
CSCuy24876	SG220 Randomly resetting
CSCuy91757	8 Ports may suddenly not work

Known Issues

The following table lists the known issues in firmware version 1.0.1.1:

Ref Number	Description
CSCun69641	All users logged in to the switch using the RADIUS server for authentication have the same privilege level (level 15), regardless of their privilege levels defined on the RADIUS server. **Workaround** None.
CSCun69651	Ingress rate limit with a small rate setting such as 512 Kbps may not take effect immediately due to the ingress bandwidth burst capability (8 MB burst size). **Workaround** None.

Related Information

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Products. No login is required.
Cisco Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Product Documentation	
Cisco 220 Series Switches	www.cisco.com/c/en/us/support/switches/small-business-220-series-smart-plus-switches/tsd-products-support-series-home.html
Regulatory Compliance and Safety Information	www.cisco.com/en/US/docs/switches/lan/csb_switching_general/rcsi/Switch_ClassA_RCSI.pdf
Warranty Information	www.cisco.com/go/warranty

P/N: OL-32794-01