

# Release Notes for the Cisco 220 Series Smart Switches Firmware Version 1.1.4.4

## August 2019

These Release Notes provide information about what's new and known issues that apply to firmware version 1.1.4.4 for the products that the following table lists:

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: 1.1.4.4
- 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

## Release Notes

---



**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.

---

## What’s New in This Release

- Energy Efficient Ethernet (EEE) is disabled on switches by default to improve interoperability between devices.
- When you first log in to a device after you complete an upgrade to this release, you must change the default username **cisco** and the default password **cisco**, unless the username and password were intentionally configured to these values before you logged in.
- You cannot remove or delete the last privilege level 15 username and password.

## Known Issues

The following table lists the resolved issues in firmware version 1.1.4.4.

:

Bug ID	Description
CSCvo66557	Command injection vulnerabilities in Sx220 switches
CSCvo78300	Sx220: Unauthenticated access to CGIs
CSCvo78320	Stack overflow vulns in various CGI scripts
CSCvo78521	HTTP ETag allows release fingerprinting
CSCvq31954	Evaluation of Sx220 Switches for TCP SACK vulnerabilities

## Related Information

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

## Release Notes

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2019 Cisco Systems, Inc. All rights reserved.