Release Notes for the Cisco 220 Series Smart Switches Firmware Version 1.2.1.2

September 2021

These Release Notes provide information about what's new and known issues that apply to firmware version 1.2.1.2 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

NOTE Please back up your configuration prior to migrating to a newer version due to possible configuration loss during the downgrade process.

Resolved Issues

The following table lists the resolved issues in firmware version 1.2.1.2

Bug	Description
CSCvx09227	SG220: Some phones may not receive proper VLAN assignment

The following table lists the resolved issues in firmware version 1.2.0.6

Bug	Description
CSCvx79184	SNMPv3 user disappear after reboot
CSCvw24834	Sx220: Access Profile Network Mask accepting wildcard mask
CSCvx57830	Sx220 - Cisco SG220-26 XSS vulnerabilities
CSCvx57925	Cisco Sx220 weak session management vulnerability
CSCvx57935	Cisco Sx220 Authenticated User Arbitrary Commands Execution

The following table lists the resolved issues in firmware version 1.1.4.5

Bug	Description
CSCvq76720	Sx220: Default private key in Cisco 220 series switches release 1.1.4.1

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	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