ZYXEL

Software Release Note
NebulaFlex Switch XGS2220-30F

Date: Sept. 16, 2024

Zyxel NebulaFlex Switch XGS2220-30F V4.90(ABYE.0) 20240916-KR Release Note

Date: September 16, 2024

This document describes the features in the XGS2220-30F for its 4.90(ABYE.0) 20240916-KR release in standalone mode.

Supported Platforms

Model	Firmware	Boot Version	Firmware Checksum
XGS2220-30F	4.90(ABYE.0) 20240916-KR	V1.00 | 06/13/2022	7808f95806af983a081f71ee7 04daf729257149b695897fa1 c0e0b4fd092cde8

New Feature and Enhancements

New Feature and Enhancement

1. [1.1.1] Enhance security by forcing users to change the password after first login on webGUI and console (eg. Telnet, SSH).
2. [1.2.1] Support password complexity feature to strengthen security, including the admin account.
3. [1.3.1] Support user IP lockout functionality after a certain number of failed login attempts.
4. [1.4.1] When entering a password in the CLI during configuration, the password should be hidden, including enable, admin, and account user modes.
5. [1.5.1] Strengthen "Password Encryption" feature with SHA256 hash algorithm for login and enable password.

6. [1.5.2] Support SNMPv3 user password encryption with AES256 hash algorithm by enabling the "Password Encryption" feature.
7. [4.1.2] Support password complexity feature to strengthen security for SNMP
8. [4.2.2] The firmware is encrypted using the SHA256 algorithm.
9. [7.1.3-1] The HTTPS private keys are now hidden and will not be displayed in the CLI.
10. [7.1.3-2] Removed unsupported HTTPS cipher suites.

- Now only supporting: ECDHE-RSA-AES256-GCM-SHA384 (0xC030) and DHE-RSA-AES256-GCM-SHA384 (0x009F)

11. [7.1.4-1] The SSH private keys are now hidden and will not be displayed in the CLI.
12. [7.1.4-2] Support re-generable SSH key(fingerprint values) for RSA only.
13. [8.1.1] Add new system log for changes in service access control configuration.
14. [8.3.1] Support event log and SNMP trap functionality to generate alerts when system logs reached 90% of thresholds.
15. [8.4.1] Limit login accounts with privileges 0 to 2 only to display basic system information on webGUI

Bug fix

	Bug fix	Nebula	Standalone
1.	CVE-2021-23840	V	V
2.	CVE-2021-3712	V	V
3.	CVE-2021-23841	V	V
4.	CVE-2022-43393	V	V
5.	CVE-2022-0778	V	V
6.	CVE-2023-0215	V	V
7.	CVE-2023-5678	V	V
8.	CVE-2023-3817	V	V
9.	CVE-2023-2650	V	V
10.	CVE-2023-0464	V	V
11.	CVE-2023-0286	V	V
12.	CVE-2023-0466	V	V

	Bug fix	Nebula	Standalone
13.	CVE-2023-0465	V	V
14.	CVE-2023-3446	V	V
15.	CVE-2024-0727	V	V
16.	CVE-2024-5535	V	V

Limitation of Settings:

	Limitation of Setting	Nebula	Standalone
1.	802.1Q Static VLANs	1K	4K
2.	Static MAC forwarding entry	-	256
3.	MAC filtering entry	256	256
4.	Cluster member	-	24*
5.	IP routing domain	32	32
6.	IGMP Filtering entry	256	256
7.	IGMP MVR entry	-	256
8.	Protocol based VLAN entries per port	-	7
9.	Port-security max address-limit number	16K	32K
10.	Syslog server entry	2	4
11.	IP source guard entry	128	512
12.	IP subnet based VLAN entry	-	16
13.	MVR VLAN entry	-	5
14.	VLAN-stacking Selective QinQ entry	-	128
15.	VLAN -mapping entry	-	128
16.	MAC table	32K	32K
17.	Routing table	64	64
18.	DHCP snooping binding table	-	16K
19.	Multicast group	1K	1K
20.	ACL	128	384
21.	DHCP option 82 profile	-	130
22.	static ARP entry	-	256
23.	Static route max entry	64	64
24.	MAC-based VLAN	-	512

25.	Voice VLAN OUI entry	6	10
26.	ZON neighbor per-port maximum clients	-	10
27.	IPv6 source guard binding table	-	50
28.	Queue	6	8

*Do not support it in stacking mode.