Versionshinweise für ER7206(UN) v2.0/v2.20/v2.26/v2.6

1). Versionsinfo: Angepasstes Modell: ER7206(UN) v2.0/v2.20/2.26/v2.6 Vollständig angepasste Controller-Version: SDNC 5.13.

Mindest-FW-Version für das Update: 2.0.0 Build 20230515 Rel.81487 und höher.

2). Verbesserungen:

1). Die Topologieidentifikation wurde optimiert.

3). Fehler behoben:

1). Es wurde das Problem behoben, dass bei Inkrafttreten des Backup-WAN der DNS nicht verfügbar war, wenn für das primäre WAN und das Backup-WAN derselbe DNS festgelegt war.

2). Das Problem wurde behoben, dass der DNS-Server nicht erreichbar war, wenn sich der DNS-Server im selben Netzwerksegment wie der WAN-Port befand.

3). Das Problem wurde behoben, dass URL-Filter und DPI nicht wirksam wurden, wenn der Browser die hybridisierte Kyber-Unterstützung mit TLS 1.3 aktivierte.

4). Das Problem wurde behoben, dass Wireguard VPN-Einträge erhalten blieben, selbst wenn der VPN-Status außergewöhnlich war.

5). Behobene Sicherheitslücke: CVE-2024-21827.

6). Das durch DPI verursachte Speicherverlustproblem wurde behoben.

7). DPI würde bei der neuesten Edge-Browserversion nicht wirksam werden.

8). Durch SNMP verursachtes Speicherverlustproblem behoben.

9). Es wurde das Problem behoben, dass bei aktivierter entsprechender Portweiterleitung der Fehler „Refer Check Failed“ gemeldet wurde, wenn versucht wurde, über den WAN-Port auf die Verwaltungsseite zuzugreifen.

10). Das Problem wurde behoben, dass der Gateway-SFP-Port keine Verbindung mit dem PON-Port OLT-P7001-8 herstellen konnte, wenn beide als Gigabit Full konfiguriert waren.

11). Das Problem wurde behoben, dass der gesamte Datenverkehr nach der Einrichtung von Wireguard VPN durch den VPN-Tunnel geleitet wurde.

12). Das Problem wurde behoben, dass die Verwaltungsseite über HTTPS-Zugriff langsam geladen wurde, wenn Browser mit Chrome-Kernel verwendet wurden.

13). Behobene Sicherheitslücke: CVE-2024-42925 (Reserviert).

14). Das Kompatibilitätsproblem mit dem neuesten OpenVPN-Client wurde behoben.