Version Info:

Adapted Model: ER7206(UN) 2.20 and 2.26, ER7206(IN) 2.28.

Minimum FW Version for Update: 2.1.2 Build 20240324 Rel.46738 and above, for downloading of any firmware version, please refer to Omada Download Center.

This is a transitional firmware for RED certification compliance which is not complied to RED certification, to fully comply to RED certification, it is recommended to upgrade to version 2.2.3 afterwards.

Once upgraded to version 2.2.2, you will not be able to downgrade to previous version. Contact Omada technical support if downgrade is required.

Enhancements:

1. Adapted to the new Omada VI.
2. Added LAN & WAN conflict resolution, logs are now reported when conflicts are detected.
3. RED certification – address four findings:
   a) Enforce strong passwords for web login.
   b) Updated the software signing algorithm to a more secure one.
   c) Disable production-test services in factory mode.
   d) Log any change to privacy assets stored on the device.

Bug Fixed:

1. Fixed security vulnerabilities:
   a) Injection flaw in DNS proxy_security.
   b) Injection flaw in sysauth.
   c) Injection flaw in WireGuard VPN.
   d) Remove hidden root-SSH capability in CLI_server binary.
   e) Eliminate legacy ecsp v1 code.
   f) Add hash-value verification to device-controller communication to prevent bypassing the integrity check.
   g) Prevent TLS hijacking via local-controller certificate.
2. Resolved functional issues:
   a) Fixed the issue that the DHCP address pool exhaustion in specific scenarios did not trigger log reporting.
   b) Fixed the issue that the L2TP server process occasionally crashed.
   c) Fixed the issue that IPS abnormally exited and generated coredump files, causing memory exhaustion.

d) Fixed the issue that static route entries whose name field contained special characters failed to take effect.

e) Fixed the issue that iOS clients occasionally caused address-pool leaks when connecting to the L2TP server.