

Version Info:

Adapted Model: DR3650v(EU) 1.0.

Fully adapted to Omada Controller V5.15.20.

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 1.1.1 afterwards.

Once upgraded to version 1.1.0, you will not be able to downgrade to previous version. Contact Omada technical support if downgrade is required.

Modification:

1. Remediate two Portal-related security vulnerabilities.
2. RED certification – address four findings:
 - a) Enforce strong passwords for web login.
 - b) Replace software signing algorithm.
 - c) Disable production-test services in factory mode.
 - d) Log any change to privacy assets stored on the device.
3. First-round security feedback – resolve two issues:
 - a) Injection flaw in DNS proxy_security.
 - b) Injection flaw in sysauth.
4. Second-round security feedback:
 - a) Injection flaw in WireGuard VPN.
 - b) Remove hidden root-SSH capability in CLI_server binary.
 - c) Eliminate legacy ecsp v1 code.
 - d) Add hash validation for device–controller exchanges.
 - e) Prevent TLS hijacking via local-controller certificate.
5. Do not pre-fill default Wi-Fi passphrase “wpapass1” in SSID configuration.

New Features:

1. SD-WAN
2. Domain name supported for OpenVPN and Wireguard VPN
3. Virtual WAN
4. Disable NAT
5. Google LDAP
6. LAN DNS
7. FQDN/Wildcards WAN DHCP Option

Enhancements:

-
1. Optimized CPU utilization.
 2. Optimized the time to enable backup link.
 3. Optimized booting time.
 4. Optimized the time to dial up the WAN link.
 5. Optimized the time to upgrade FW.
 6. Optimized the time to generate OpenVPN profile.

Bug Fixed:

1. Fixed the HTTPS redirection exception in standalone mode.
2. Fixed the issue where the static route for L2TP VPN doesn't take effect after reenabling L2TP VPN.
3. Fixed the WOL exception when dropping some unknown unicast packets.
4. Fixed the issue where the PPTP VPN would occasionally disconnect.
5. Fixed the issue of DNS abnormal in specific scenario causing adoption failure.