

TCR100 Firmware Downloads

[Main Page](#) > [TCR Routers](#) > [TCR100](#) > **TCR100 Firmware Downloads**

This page contains firmware files for TCR100 devices. Look to the table below or the [changelog](#) to find download links.

To upgrade firmware using WebUI, follow the instructions in [TCR100 Firmware](#).

File	Type	Release date	Size	MD5	Changelog
TCR1_R_00.07.07.3_WEBUI.bin	Latest FW	2024.06.25	11.69 MB	9a06ab2b888d07c9665790f7738ab887	Link
TCR1_R_00.07.05.4_WEBUI.bin	Mass production FW	2023.11.09	11.13 MB	ab475a5d3564755c1d4207a8cd7ae8a3	Link
TCR1_R_GPL_00.07.07.3.tar.gz	SDK	2024.06.25	19.75 MB	69ea433b1eb10b7d595d6d9abdb14d07	

Note: packages for [Package Manager](#) are independent from firmware and can be downloaded in the [Package Downloads](#) page.

FW checksums

Checksums for firmware files can be found [here](#).

Changelog

[TCR1_R_00.07.07.3](#) | 2024.06.25

- **Fix**
 - **Network**
 - WebUI: fixed port advertisement change
 - **System**
 - FOTA: fixed config when upgrading from older firmware with keep settings
 - **CVE Patches**
 - CVE-2024-31950
 - CVE-2024-31951
-

[TCR1_R_00.07.07.2](#) | 2024.06.12

- **Improvements**
 - **Network**
 - Zerotier: added backup WAN interface blacklisting if WAN failover is enabled
 - Mobile: improved communication stability with eSIM

- **Services**
 - SNMP: added bruteforce attack prevention when using SNMP v3 user
 - L2TP: improved reconnect attempt logic
 - Wireless: removed unnecessary information from system logs
 - **System**
 - SSH: removed weak SSH algorithms
 - Telnet: moved to Package Manager
 - **Fix**
 - **Network**
 - BGP: fixed instance migration issues
 - Mobile: fixed forced APN configuration
 - **Services**
 - DMVPN: fixed duplicate NHRP map entries creation
 - OpenVPN: added fixes for the insecure tls-cert-profile option usage
 - **System**
 - IP Block: fixed blocking of UDP traffic
 - Ledman: fixed WiFi LED indication when WiFi configuration is changed
 - Uboot: fixed firmware recovery update via uboot on Windows
 - **CVE Patches**
 - CVE-2024-31948
-

[TCR1_R_00.07.07.1](#) | 2024.05.03

- **New**
 - **Network**
 - WebUI: added ESM/EMM message notifications
 - WebUI: added internet status tracking configuration and overview widget
 - LAN: added a new IPv6 LAN status page
 - Static Leases: added a new IPv6 Static Leases page
 - WebUI: added custom domain name resolve option in “DNS” configuration page
 - Auto APN: added “uno.au-net.ne.jp” APN for “KDDI” operator
 - Auto APN: added 'eprivate010.tisparkle.com' APN for “Sparkle” operator
 - QoS: added mobile interface select option
 - Mobile: improved connection establish time for uqmi protocol
 - Failover: added additional connection flush options
 - Wireless: added auto-reconnect disable functionality
 - Wireless: added ability to use PKCS#12 certificates for EAP-TLS authentication
 - VRF: added initial Virtual Routing and Forwarding support
 - **Services**
 - DLMS Client: added persistent TCP connections
 - Events Reporting: added unexpected shutdown event
 - Modbus Client: added 64bit data types
 - IPPerf3: added iPerf3 to Package Manager
 - TR-069: added PCI, LAC, TAC, EARFCN and Neighbour cells data to Device.MobileInfo node
 - Hotspot: added domain and subdomain options for external landing page
 - **System**
 - WebUI: added the ability to generate random passwords for password input fields
 - WebUI: added reset to “Factory defaults” option

- System: changed firmware certificate verification tool
- IP Block: added time-based login attempt blocking
- WebUI: added firmware update notification support
- PAM: added the ability to set port for TACACS+
- Logging: added multiple remote syslog servers support

- **Improvements**

- **Network**

- Static Leases: added possibility to use MAC with wildcard
- WebUI: added ability to disable modem update notifications
- Topology: changed network devices scanning application
- WebUI: improved design of Status - LAN page
- DHCP: simplified DHCP configurations in other pages and moved full DHCP configuration to a separate page
- WDHCP: removed default disabled server configuration for WAN interface
- WebUI: simplified data entry of DNS forwardings by separating hostname and IP address fields
- BGP: added Virtual Routing and Forwarding (VRF) support
- BGP: added multiple BGP instance support
- WebUI: adjusted responsive design breakpoints
- WebUI: added additional field for warning threshold to allow entering value as percentage in Mobile Data Limit section
- Mobile: improved mobile services stability when SIM card is lost during SMS sending
- Mobile: updated bridge/passthrough mode logic to flush ARP and add static ARP entry if MAC is specified
- Mobile: improved SIM switch logging and protection on failure to acquire data
- WebUI: added partial data loading to APN database page
- Mobile: improved SMS sending timeouts during network issues
- Mobile: improved connection handling when data limit is reached
- Mobile: added metric to default gateway when using passthrough mode
- WebUI: added validation for 2 same APNs
- WebUI: updated Band selection field to show duplex modes in Mobile General page
- WebUI: added an information icon and disabled delete button for wireless instance when it is associated with a hotspot interface
- Wireless: improved hidden AP handling when showing scan results
- Wireless: added a range of channels to 5 Ghz radio to use as fallback if it drops after radar detection when using DFS channel
- Dnsmasq: updated dnsmasq to version 2.89

- **Services**

- Wireguard: added option to bind tunnel to a specific interface
- OPC UA Client: added limits (10 servers, 20 groups, 50 nodes per server, 50 values per group)
- DLMS Client: increased maximum count of connection sections to 30
- DLMS Client: added short name referencing
- SNMP: set strict default community access when IPv6 address is used
- SNMP: improved sysName OID to set device's hostname
- Auto Reply: added available SMS message parameters to "Message text" input
- Modbus Client: allow using diacritics in SMS alarms
- Hotspot: moved MAC blocking option from Access Control to Hotspot page
- WebUI: added MAC authentication support when using RADIUS authentication

mode

- WebUI: moved licenses to footer
- OpenVPN: added the bridge option for selecting the network device to be bridged with
- OpenVPN: added possibility to create more than one TAP client
- SSTP: updated package version to 1.0.19
- Mosquitto: updated package version to 2.0.17

◦ **System**

- WebUI: added more strict password requirements for restoring backup
- SMTP: added option to either not verify SMTP server or upload SMTP server's CA file to verify authenticity
- WebUI: Added the ability to choose the ROOT CA when using certificates from the device
- WebUI: unified time format to ISO8601 across the entire WebUI
- WebUI: added ability to choose imported certificate and key as 'Server certificate' and 'Server key' in 'Access Control'
- WebUI: added 'Hosts' and 'IP Addresses' options for 'Simple' certificate generation and certificate signing
- WebUI: changed firmware update option to server as a default option
- WebUI: improved first login password change logic
- Certificates: updated Root CA certificates
- GPL: added offline package preparation command for GPL builds
- Speedtest: added multiple connections support to improve accuracy
- Libcap: updated package version to 2.69

• **Fix**

◦ **Network**

- Topology: fixed showing interfaces with assigned VLAN
- WebUI: fixed static routing creation for GRE instance
- Network: fixed DHCPv4 relay mode enabling
- Mobile: fixed PIN code set after modem restart
- Mobile: fixed cases where 5G NSA network type was shown incorrectly
- Mobile: fixed an issue where using SIM change command on one SIM slot modems would reset connection
- Mobile: fixed an issue where message storage would not be checked correctly
- Mobile: fixed temperature value sometimes returning 0
- Mobile: fixed denied roaming flag set
- Mobile: fixed issue where RSSI value was displayed as 0 when using 2G/3G network types
- Failover: fixed Failover missing active rules when using multiple source and destination IP addresses
- Failover: fixed an issue where failover would not function correctly while using a mobile interface
- Failover - WebUI: fixed network and failover interface metric sorting synchronization issue
- Failover - WebUI: fixed failover rule policy save issue with newly added WAN interface
- Interfaces: fixed failover value for new WAN being taken from WAN that was just deleted
- Wireless: fixed Wifi Scanner not saving scanned WiFi SSIDs
- Wireless: fixed missing CCMP-256 and GCMP-256 cipher types in scan results
- Wireless: fixed missing GCMP-256 cipher when using WPA3-EAP encryption in

Client mode

- Wireless: fixed skipped MAC address value for interface in Client mode
- Wireless - WebUI: fixed mesh nodes not being shown in Status->Wireless->Interfaces page
- Wireless - WebUI: fixed proposed configuration settings when connecting to a mesh point network
- MultiAP: fixed client not switching to another AP if incorrect password was provided

◦ **Services**

- Modbus Client: allow using negative floating point values in requests
- Azure IoT Hub: fixed Data to Server minor WebUI dependency bugs
- Data to Server: fixed DLMS data formatting
- Data to Server: fixed Network link state data display
- DLMS Client: fixed segfault while reading profile generic COSEM object
- DLMS Client: fixed profile generic entries reading
- DLMS Client: fixed application memory allocation issues
- SSTP: fixed route adding when default route is enabled
- SNMP: fixed VLAN OID naming
- OpenVPN: added fixes for instance status tracking functionality
- OpenVPN: resolved uptime counting issues
- PPTP: fixed PPTP instance deletion problem
- Azure IoT Hub: fixed 'contentType' telemetry message parameter
- Hotspot: fixed password validation for locally created users and signed-up users
- Hotspot: fixed session invalidation after deleting registered user
- Hotspot: fixed SMS OTP password reuse
- Hotspot: fixed firewall rule creation
- PPTP: fixed problem related with routes when failover is enabled
- Modbus Client: fixed issue where service freezes when SMS alarm is sent
- UPnP: updated package version to 2.3.4

◦ **System**

- Mobile - NTP Client: fixed 'Count of time synchronizations' execution when synchronization to mobile operator is chosen
- Package Manager: fixed spinner message when restarting network after package upload or download
- Package Manager: fixed supported devices check when installing a package from server
- WebUI: fixed language install from uploaded package after upgrade with keep settings
- WebUI: fixed an issue when a user was not logged out after changing profiles
- Telnet: fixed segmentation fault during concurrent connections
- CLI: fixed enter key issue on mobile chromium based browsers
- System Users: fixed SSH session close after deleting user or disabling SSH access
- Profiles: fixed profile migration with installed packages
- WebUI: fixed Hotspot log page table search functionality
- Speedtest: fix missing download speed on some servers
- PAM: updated libpam to version 1.6.0

• **CVE Patches**

- CVE-2022-4603
- CVE-2022-23308
- CVE 2022-45061
- CVE-2023-0466

- CVE-2023-6129
- CVE-2023-7042
- CVE 2023-24329
- CVE 2023-27043
- CVE-2023-42366
- CVE-2023-46218
- CVE-2023-46219
- CVE-2023-46752
- CVE-2023-46753
- CVE-2023-48795
- CVE-2024-2397
- CVE-2024-25062
- CVE-2024-27913
- CVE-2024-22365

TCR1_R_00.07.06.3 | 2024.01.17

Note: Firmware version *TCR1_R_00.07.06.3* was removed due to an issue with mismatching wireless SSID between device housing label and default device SSID on factory configuration.

[TCR1_R_00.07.05.4](#) | 2023.11.09

- **Improvements**

- **WebUI**

- Improved asynchronous pagination in events log pages
- Optimized Overview page load
- Added resource loading cancellation after switching to different page

[TCR1_R_00.07.05](#) | 2023.10.09

- **New**

- **Network**

- Added "shared.m2m.ch" APN for Swisscom IoT operator to APN database
- Added "gamma" APN to auto-APN database
- Added "soracom.io" APN for Soracom operator to APN database
- Added "simbase" APN to auto-APN database
- Added "pnd" APN for Pond IoT to auto-APN database
- Added "spitfire1" APN for Spitfire operator to APN database
- Software Offloading enabled on default configuration
- New argument in "gsmctl" CLI command for Carrier aggregation
- Numeric mode support for modem AT commands
- Enabled dynamic MTU configuration on mobile interfaces by default
- WDS support for wireless bridging

- **Services**

- DLMS Client package
- 7zip package
- TincVPN package
- Added router uptime and mobile connection uptime data parameters to SNMP
- Custom MQTT publisher/subscriber topics definition support
- Alternative configuration file upload support for MQTT Broker service

- Device Provisioning Service support for Azure IoT Hub service
- Added more mobile usage parameters to SNMP
- **WebUI**
 - Firewall status page
 - Page search feature
 - Network Topology page
 - "Allow insecure connection" option for MQTT TLS protocol in Data to Server service
 - Package Restore feature Enable/Disable option
 - Hotspot client connection/disconnection trap option for SNMP service
 - Added Events log trap option for SNMP service
 - Confirm dialog when cancelling a verified package in Package Manager
 - "Bridge ALPN" option for Bridge configuration in MQTT Broker service
 - New subtypes of events that specify a specific port on "Events Reporting" and "SNMP Trap rules" pages
 - Specific firmware packages repository link in Package Manager page
 - Ability to enter decryption passphrase for encrypted private keys
 - "Reconnect" button in RMS page
 - New event "Device startup completed" in Events Reporting service
 - Port status and configuration page
 - Wireless interface QR code generator
 - Channel analysis page Status -> Wireless -> Channel Analysis
 - Disabled direct network interface deletion when it is associated with a wireless interface
 - Limited to a single section configuration and added IP address field for Relayd service
 - "Fast roaming" configuration for Wireless service in Client mode
 - Updated Status->Network->Wireless page to display interfaces as cards and added ability to filter connected clients by selected interface
 - Modem Debug page
 - APN database management page added to package manager
 - Added "Message forwarding" option in SMS Rules page when rule type is "Execute custom script"
 - Ability to unblock SIM card and insert SIM PIN in Overview page
 - New SMS rules "Reset mobile connection" and "Reload config"
 - "SMS limit clear due" display in Overview page
 - Added modem temperature to System -> Status page
 - IP6 table configuration option for DHCPv6 protocol in Network -> WAN page
- **System**
 - Mechanism to rebrand WebUI using GPL
 - Possibility to create web applications with closed-source GPL
- **Improvements**
 - **Network**
 - Moved FRR VTYSH package to package manager
 - Made newly created Firewall Traffic, NAT rules and Port Forwards disabled by default
 - Improved Interfaces to enable IPv6 DHCP server when mobile v6 or v4v6 PDP type is set
 - Improved auto APN selection
 - SMS sending event is now logged into events log

- Improved roaming control
- Removed unused APN usernames and passwords from auto-APN database
- Added connection to the operator when no mobile interfaces are active
- Improved VoLTE management functions
- Improved cases where Low Signal Reconnect sometimes executed prematurely
- Improved wrong SIM PIN remove logic
- Added automatic reconfiguration when switching between wireless interface modes
- Added automatically generated name option for new network
- Updated default subnet to 192.168.3.0/24 for Guest Network
- **Services**
 - New reworked Data to Server
 - UPNP moved to package manager
 - Added IPv6 support for Modbus TCP Server/Client services
 - Refactored Azure IoT Hub service
 - Improved resiliency to timeouts in Modbus Client service
 - Added PDU data type to Modbus read requests
 - Added new formatters for MQTT alarms in Modbus Client service
 - Added main section to make test functions independent in Modbus Client service
 - Improved WAN IP register reading time in Modbus service
 - Sped up default profile and profile template generation for Profiles functionality
 - Optimized profile change time for Profiles functionality
 - Added IPv6 support for Stunnel VPN
 - Added MAC blocking for client connections after set amount of failed login attempts in Hotspot service
 - Improved TCPdump by allowing to capture packets from any interface
 - Added OSPF support for DMVPN
 - Updated Hotspot password hashing to sha512
 - A single SMS message with multiple PDUs is sent instead of multiple SMS messages in Email to SMS service
 - Allowed connection to SMPP server using IPv6 address
 - Extended IP unblock action functionality in SMS Utilities
 - Increased allowed Email to SMS service message size to 61440 bytes
 - Added I/O pin name to trap notification message
- **WebUI**
 - Reorganized menu
 - Updated header design
 - Split Interfaces configuration in Advanced mode into two pages: WAN and LAN, identically as in Basic WebUI mode
 - Moved Interfaces IPv6 configuration into separate tab
 - Added client/server status information in OpenVPN instance overview page
 - Added more IPv6 information to interface status in Interfaces page
 - Removed "Custom delegated IPv6-prefix" field from DHCPv6 configuration in Interfaces page
 - Disabled DHCPv6 interface editing while in basic mode
 - Refactored custom DHCP options into separate modal
 - Added automatic start and end IP allocation for DHCP server configuration in Interfaces
 - Added client/server status information in L2TP VPN page
 - Added "MTU" field to L2TP client configuration page
 - Added CHAP, PAP and MSCHAP-v2 authentication fields to L2TP instance

configuration

- Added more detailed IPsec VPN status information
 - Encryption AES-256-CBC added as default in OpenVPN
 - Added "Authentication algorithm" support to OpenVPN configuration with static key mode
 - Added GRE (DMVPN) VPN tunnel source support to any instead of specific interface
 - Improved Hotspot landing page theme package removal
 - Added upload and download theme functionality to Hotspot Landing page
 - Improved ZeroTier VPN bridge configuration
 - Added ability to adjust order of rules in Firewall page
 - Added IPv6 RAW table to be displayed in Status -> Firewall
 - Improved file upload component's visual appearance
 - Change "Allow anonymous" option default value to 0 in MQTT Broker
 - Added option to specify "Client ID" in MQTT Publisher
 - Added functionality to select specific interface in Web Filter service
 - Allowed to select FTP server subfolder in Traffic Logging service
 - Renamed various service master/slave naming convention in config files, package names and webUI to client/server
 - Added "Create static" button in Status -> Network -> LAN which bind DHCP lease for device
 - Updated Status -> Network -> Mobile page layout
 - Added bandwidth, provider in Status -> Network -> Mobile page
 - Added colors for signal strength values in Status -> Network -> Mobile page
 - Added frequency, pcid, mcc, mnc and LAC values in Status->Network->Mobile page
 - Refactored network type selection in Network -> Mobile -> General page
 - Serving cell information is not returned anymore when SIM card is not inserted
 - Changed default "Check interval" option value in Network -> Mobile -> SIM Switch page
 - Added button in a Scanned operators table which allows to add an operator to the operator list
 - Added search bar in Mobile Utilities -> SMS Utilities page
 - Added SMS sent and limit count to Network -> Mobile -> General page
 - Updated Mobile Signal graphs to show EC/IO and RSCP values when network type is 3G
 - Added DFS channel marking in Network -> Wireless
 - Show wireless MAC address even when interface is inactive in Status -> System page
 - Merged Multi AP configuration to wireless interface edit modal
 - Added automatic network switch to bridge if selected in Wireless configuration
 - Added default encryption for newly created wireless interfaces
 - Simplified "802.11r Fast Transition" configuration options in Wireless interface configuration
- **System**
 - Updated kernel version to 5.4.251
 - Updated UCI version to 2021-10-22
 - Updated SSHFS version to 3.7.1
 - Updated FRR suite to 8.4.2
 - Updated cURL version to 8.2.0
 - Updated TCPdump version to 4.99.4

- Updated C-ares version to 1.19.1
- Updated iproute2 version to 5.19.0
- Updated libubox package version to 2021-08-19
- Added CVE patch CVE-2023-2650
- Added additional firmware information in CLI prompt banner
- Connection mode LED now blinks on data transfer
- Changed "routername" to "devicename" in system config file
- Made all clients get disconnected out once dropbear service is disabled
- Improved firmware downgrade restrictions for certain regions
- Device name is now displayed in browser tab when in WebUI login page
- Added NF conntrack information in generated troubleshoot archive

- **Fix**

- **Network**

- Fixed UDP Broadcast Relay service crashing on start without physical network device
- Fixed SMS limit period migration
- Fixed SMS limit size breaking various functionality
- Fixed custom IPv6 DNS option not overriding default DNS from operator
- Fixed an issue with blacklist and whitelist connection
- Fixed multipart SMS handling
- Fixed wrong SIM state display when SIM is fully blocked
- Fixed incorrect virginmobile APN MNC
- Fixed mobile operator scanning fault when no mobile interfaces are active
- Fixed mobile interfaces generating multiple events on mobile connection
- Fixed PDU SMS parsing when operator provides user data header in single part SMS
- Added scheduled data limit clear for inactive mobile interfaces
- Fixed wrong or empty WAN state info
- Fixed Wireless AP and STA functionality for 5GHz band
- Fixed Wireless scanning issue with certain configuration
- Fixed Wireless transmit power changing without user input after saving different country code
- Fixed clients isolation functionality in Wireless
- Fixed Wireless STA authentication failure in case of channel change
- Fixed Multi AP startup when changing Multi AP configuration in Wireless
- Fixed client connection to EAP Wireless network
- Fixed connection tracking for main interface in Failover

- **Services**

- Fixed reconnecting to inactive connections for Modbus Server service
- Fixed Modbus Client response after reboot write request
- Fixed Modbus Server to show error when trying to get operator name without SIM
- Updated Modbus Client to handle large numbers of schedule rules, when frequency is set to schedule (Daini)
- Fixed "Input" rule displaying incorrect and missing ports in Network -> Firewall -> Traffic Rules
- Fixed WireGuard VPN endpoint resolving problem
- Peer cache is no longer deleted when ZeroTier service is restarted
- Fixed RMS data collection about the list of devices connected to WiFi
- Fixed showing incorrect Internet state in RMS
- Fixed WiFi client info display in RMS

- Implemented error handling when device is blocked or unrecognized by RMS
 - Fixed L2TP client sometimes not adding routes on successful connection
 - Fixed NTP time sync with browser functionality in some edge cases
 - Fixed reinstalled packages" verification when device name is changed
 - Fixed an issue where signal query would return invalid value instead of error in case of no signal in MQTT Publisher service
 - Fixed OpenVPN firewall rule creation for both IPv4 and IPv6
 - Fixed OpenVPN server crash loop after changing authentication from TLS to Static Key
 - Fixed IPsec VPN connection problem with small lifetime values
 - Fixed IPsec "Default Route" not working when Flow Offloading is enabled
 - Fixed an issue where system directory could be used as a mount point in SSHFS service
 - Fixed IP block feature to unblock an OpenVPN IP address on successful authentication
 - Fixed package installation process bug when packages have different architecture names
 - Added "bearer token" authentication functionality in Dynamic DNS
 - Fixed MQTT Broker "local_port" option keep settings migration
 - Remove public keys when key-based authentication is disabled in Access Control
 - Fixed "Parity" field "Mark" and "Space" options being ignored in DNP3 Serial services
 - Corrected SNMP MIB file syntax according to standards
 - Fixed returned port count in SNMP
 - Fixed disabled CLI remote access taking up a session slot
 - Fixed received SMS messages parsing with trailing whitespaces
 - Fixed VPN status rule message text in SMS Utilities
- **WebUI**
- Fixed empty events cards in Overview page when no content is available
 - Fixed modal form inputs not clearing upon closing after nested modal is saved
 - Fixed select menu closing when selecting custom option
 - Fixed multi select expanding table row when adding new values
 - Fixed global section caching after deleting a section in a table
 - Fixed unpredictable search logic in tables
 - Fixed interfaces reordering by metrics in Failover page
 - Removed ability to select ports on ICMP and ESP protocol in Failover page
 - Fixed wrong status when interface is disabled in Failover page
 - Fixed firewall zone and rule creation/deletion on VPN configuration creation/deletion
 - Fixed STP enabling issue in Interfaces
 - Fixed EIGRP status info in Dynamic Routes
 - Fixed issue with custom DHCP options where you could not have multiple values per rule
 - Fixed Routing/NAT Offloading section display in Network -> Firewall -> General Settings when device is not supported
 - Fixed SSH/HTTP/HTTPS/ICMP setting in Network -> Firewall -> Attack Prevention page
 - Fixed failing Firewall rules with united protocol formats
 - Fixed zone select component not closing options menu when selecting an option in Firewall pages
 - Fixed memory leak when cancelling file uploads on Chromium-based browser

- Fixed group settings saving by removing deprecated ":section" routes in Administration -> User Settings -> System Users
- Fixed allowing IDs above 247 in Modbus Client service
- Fixed selecting SIM in Modbus Client service Alarms
- Fixed Modbus Alarm telephone number limit
- Fixed to show available options for test requests on error in Modbus Client service
- Fixed Modbus Alarm I/O pin display values
- Fixed issue when creating instance named "gre" does not show in GRE VPN
- Remote endpoint field now allows underscore character in IPsec VPN
- Fixed ZeroTier wrong service status display in Status -> Services
- Fixed problems with L2TP/PPTP VPN firewall rules automatic creation
- Fixed problem related to the enable/disable toggle in OpenVPN instance overview page
- Added fixes for key-direction missing problem when uploading OpenVPN config file
- Fixed login page read-only inputs after custom user logout
- Fixed issue when double clicking firmware upgrade cancel button returned error
- Fixed Package Manager prompt message to appear when package requires network restart
- Fixed showing in queue packages when they contained special symbols in the Package Manager page
- Fixed various visual Side Widget bugs
- Fixed Data to Server DNP3 filter from flash display
- Fixed incorrect source data displayed in Realtime Data -> Connections table
- Fixed memory expansion confirmation prompt title
- Fixed incorrect configuration saving in Hotspot 2.0 service
- Disabled password hashing for new user creation in Hotspot service
- Fixed Hotspot landing page themes saving bug
- Fixed test email sending to more than one recipient in Events Reporting page
- Fixed VLAN OID values in SNMP service
- Output proper error message in case of hardware not being supported in Firmware Upgrade
- Fixed being able to open side widget when user does not have read access
- Fixed profile creation when current configuration is not present
- Fixed wrong protocol data display in "Access control" page
- Fixed LAN interfaces not showing up before WAN interfaces in Status -> Realtime Data -> Traffic
- Fixed carrier aggregation information when no connection is made or SIM card is not inserted
- Changed representation of mobile cell ID from hexadecimal to integer type
- Fixed Mobile Utilities "SMS forwarding to HTTP" URL generation
- Fixed an issue where sometimes bands were not represented correctly on certain modems
- Fixed provider information and IMSI value representation when SIM and modem cannot provide this information
- Fixed mobile pages throwing 404 error when modem disconnects
- Fixed WebUI showing mobile connection when no SIM card is inserted
- Updated Network -> Wireless interface add and delete button visibility in basic mode
- Fixed Wireless Multi AP incorrect SSID list after removal of an instance
- Fixed MAC address filtering in Network -> Wireless page to list only connected

WiFi devices

- Fixed "Clear Collect Data" button logic to not clear overall mobile usage info
- Fixed "Used data" showing large negative numbers for disabled mobile interfaces with Data Limit enabled
- Fixed Guest Network configuration editing in Network -> Wireless page
- Fixed error when user has no write permissions in Speed Test page

◦ **System**

- Patched CVE-2023-0386 vulnerability
- Patched CVE-2023-0464 vulnerability
- Patched CVE-2023-0465 vulnerability
- Patched CVE-2023-2602 vulnerability
- Patched CVE-2023-3772 vulnerability
- Patched CVE-2023-4128 vulnerability
- Patched CVE-2023-33476 vulnerability
- Patched CVE-2023-28484 vulnerability
- Patched CVE-2023-29469 vulnerability
- Patched CVE-2023-31490 vulnerability
- Patched CVE-2021-36369 vulnerability
- Patched CVE-2023-48174 vulnerability
- Delayed Custom Scripts execution on boot, after storage devices are mounted
- Fixed Custom Scripts permissions after save
- Changed certificate expiry calculation mechanism to fix Y2K38 bug
- Fixed downloading of certificates that have a space in their name in Administration -> Certificates -> Certificates Manager
- Fixed Events Log database rotation to prevent log partition space exhaustion
- Fixed duplication and sorting of all events IDs in Events Log
- Fixed FOTA crash when current hours is with leading 0
- Fixed crontab job removal after disabling FOTA
- Changed Mosquitto build options to not include cJSON library
- Fixed device name resetting to default upon refresh in Administration

[TCR1_R_00.07.04.5](#) | 2023.07.24

- **Improvements**

- **Network**

- Added metric field support in BGP Route-maps page

- **Fix**

- **Network**

- Fixed an issue with MBN selection when device is started for the first time
- Fixed an issue where MBN activation would not be successful
- Fixed service provider parsing when operator does not provide all fields for Quectel modems

[TCR1_R_00.07.04.4](#) | 2023.06.26

- **New**

- **Network**

- Travelmate package for captive portal redirection

- **Improvements**

- **Network**

- Improved mobile operator query methods and operator name parsing in various services
 - **Services**
 - Improved UPNP lease file validation
 - **System**
 - Device name is now displayed in browser tab when in login page
- **Fix**
 - **Network**
 - Fixed a connection issue with bridge/passthrough mode when reconnecting ethernet cable
 - Fixed long mobile operator list parsing for whitelist/blacklist functionality
 - Patched CVE-2023-32233 vulnerability
 - Fixed an issue with Multi AP service remaining enabled when disabling
 - Fixed default networks in WAN firewall zone and possibility to add a network that is not yet created
 - **Services**
 - Fixed connection establishment for RMS MQTT service
 - Implemented partial restart when connection with RMS server fails
 - Fixed device name resetting to default upon WebUI page refresh
 - Fixed being able to set device name without passing validations
 - Fixed WireGuard port change in firewall traffic rule when modifying instance port

[TCR1_R_00.07.04.3](#) | 2023.05.11

- **Improvement**
 - **System**
 - Optimized firmware image size
 - Removed SSH RSA key generation
 - Added SSH ECDSA key generation
- **Fix**
 - **Network**
 - Fixed an issue with mobile when Call Utilities configuration is invalid
 - Fixed clients being unable to connect to wireless AP when multi AP configuration is empty
 - Fixed an issue where sometimes PIN/PUK code was deleted when performing a SIM switch
 - **Services**
 - Fixed incorrect mobile data usage provided to RMS service
 - **System**
 - Fixed an issue on bootloader web recovery hanging with certain firmware sizes

[TCR1_R_00.07.04.2](#) | 2023.04.18

- **New**
 - nftables support
- **Improvement**
 - **Network**
 - Added PDP profile registry and LTE SMS format functions & management for the Verizon network

- Improved SIM detection algorithm
 - Improved Multi-APN connection establishment time
- **WebUI**
 - Improved Overview page performance
- **System**
 - Changed hostname to router name
 - Updated OpenSSL to version 1.1.1t
 - Updated CA certificates to version 20211016
 - Updated libiwinfo to version 2022-08-19
- **Fix**
 - **Network**
 - Fixed IPv4, IPv6 mobile connection restarts
 - Fixed operator scanning when mobile interface is disabled
 - Fixed data limit and tracking when software flow offloading is enabled
 - Added network reload call before bringing the mobile interface up
 - Fixed Port-based VLAN ID calculation issue
 - Fixed PDP context authentication when using special characters
 - **Services**
 - Fixed event text for configurable inputs/outputs on I/O Juggler
 - Fixed I/O PIN3 value not changing via MODBUS TCP
 - Added I/O status request error handling in various WebUI pages when the I/O service is booting up
 - Fixed wrong timezone returned issue in Operator Station Synchronization & Timezone Synchronization
 - Fixed MODBUS TCP Slave memory leak issue when requesting mobile parameters
 - Fixed OpenVPN enabling/disabling when using Password or TLS/Password authentication modes
 - Fixed OpenVPN keep alive setting migration issue
 - Fixed PPTP server name setting migration issue
 - Fixed missing WebUI issue caused by Email Relay installation
 - Fixed NTP's Operator Station Synchronization memory leak issue
 - Fixed test email validation
 - **System**
 - Fixed libcares vulnerability CVE-2022-4904
 - Fixed frr vulnerability CVE-2022-37035
 - Removed ability for non root users to edit scripts that get executed as root

[TCR1_R_00.07.04.1](#) | 2023.03.24

- **Fix**
 - **Network**
 - Fixed Data Limit issue

[TCR1_R_00.07.04](#) | 2023.03.07

- **Improvements**
 - **WebUI**
 - Improved data persistence between page refreshes
 - Improved page navigation behavior
 - Improved redirect logic to open configuration edit modals
 - Updated the 'Status -> Mobile' page

- Updated interface card in the Overview page
 - Separated Sent and Received data bars on the chart in the Mobile Usage page
- **Network**
 - Added an info message displayed when a faulty SIM card is inserted
 - Added ResIOT operator's APNs to the APN database
 - Improved mobile connection re-establishment after reboot
 - Improved mobile connection recovery in cases where it was lost unexpectedly
 - Improved 'Deny data roaming' operation when switching between operators
 - Changed default WiFi AP cipher to CCMP (AES)
 - Added the logging of MAC addresses rejected by a WiFi AP
- **Services**
 - Added MQTT support to I/O Juggler
 - Added an error message when trying to send an SMS from the 'Send Messages' page with no SIM card inserted
 - Changed the behavior of setting the 'Write to config' flag in the 'mobileoff' SMS rule
 - Added argument support for the 'Execute custom script' SMS rule
 - Added a frequency option 'schedule' Modbus Master
 - Added pagination to Events Reporting overview
 - Added limit to Events Reporting rule list
 - Added email logging for Events reporting
 - 'Sync with browser' button in the NTP page now also synchronizes the time zone
 - Added a limit of 30 for NTP instances
 - Made Networks selections in the 'Traffic Logging' page to display interface choices dynamically
 - Added "make before break" option to IPsec configuration
 - Added MODBUS TCP connection handling layer to MQTT-MODBUS Gateway
 - Improved MODBUS Master connection handling to reduce connection count
 - Updated modbus request error messages
 - Added OpenVPN server ip block support
 - Added MQTT support for MODBUS Master alarms
 - Added the possibility to get the device's Ethernet port data via SNMP
- **System**
 - Updated bash to version 5.1.16
 - Added detailed FW update failure error message to Events Log
 - Improved firmware upload/validation error messages
 - Updated Turkish language support
 - Added protocol column to IP block page
 - Added "vpns.log" file to the Troubleshoot package
 - Added Wireguard tunnel information to the Troubleshoot package
 - Updated default admin group access rights
 - Updated DFOTA notification to show "More info" only when the update is forced
- **Fix**
 - **WebUI**
 - Fixed MAC address showing on mobile interfaces
 - Fixed mobile cell ID displaying in hexadecimal
 - Fixed mobile data limit card creation in the Overview page
 - Fixed modem widget disappearing from the Overview page
 - Fixed Services page not displaying data after Thingworx package is installed
 - **Network**

- Fixed interface priority change issue
- Fixed a Custom Firewall Rule editing issue
- Fixed DMZ configuration saving while it is disabled
- Fixed Port Scan script execution failure
- Fixed Firewall zone duplication issue
- Fixed call function when VoLTE is disabled
- Fixed VoLTE control when IMS is not enabled
- Fixed mobile IPv6 IP checking when the device didn't get a correct IP address
- Fixed APN authentication when using empty credentials
- Fixed manual APN selection from list
- Fixed disabled WiFi interface after factory reset
- Fixed WiFi interface creation with SAE mixed encryption
- **Services**
 - Fixed I/O Scheduler overlapping instances issue
 - Fixed Input/Output image pin colors
 - Fixed issue that causes ADC subscribers to receive notifications for when ACL is active
 - Fixed WiFi Hotspot landing page uploaded theme image display
 - Fixed WiFi Hotspot trial user deletion issue
 - Fixed WiFi Hotspot service crash when associated WiFi interface is not up
 - Fixed WiFi Hotspot password request by SMS
 - Fixed WiFi Scanner starting process when the WiFi interface is disabled
 - Added limitations on message size and quantity of email messages in Email to SMS
 - Fixed SMTP HELLO value parsing issue
 - Fixed SMS message window reset button
 - Fixed not being able to save empty 'Message text' field in Auto Reply
 - Fixed multi-part SMS concatenation
 - Fixed multi-part SMS processing
 - Fixed SMS error message on 'Mobile Data Reset' action
 - Fixed Data To Server JSON format %n, %N and %s flag issues
 - Fixed Events Reporting email data clean
 - Fixed Events Reporting missing config selections
 - Fixed GRE Tunnel's 'Tunnel source' field validation when the source is custom
 - Fixed IPsec instance deletion after removing DMVPN package
 - Fixed IPsec migration via Backup file when DMVPN is configured
 - Fixed IPsec naming issue when the includes an equals sign
 - Fixed L2TP client to use correct interface on failover events
 - Fixed L2TP over IPsec connection dropping issue when connecting from a Windows client
 - Fixed MODBUS database size limiting issue
 - Fixed MODBUS MQTT Gateway client ID input
 - Fixed MODBUS TCP Slave RSSI value
 - Fixed MODBUS test button returning errors when several non-connected devices are configured
 - Fixed NTP Etc/GMT+1 and Etc/GMT-1 time zones
 - Fixed OpenVPN password validation when no CA certificate is uploaded or 'custom' template is selected
 - Fixed OpenVPN Static Key configuration saving by making Static key upload required
 - Fixed OpenVPN TLS client creation issue while LAN is down
 - Fixed Package Manager displaying non-existent packages

- Fixed Package Manager errors showing up after successful installations
- Fixed Periodic Reboot entry duplication after a power cycle
- Fixed PPTP 'Client to client' option not being applied after save
- Fixed receiving excessive device state emails after a reboot is initialized over RMS
- Fixed WebUI unavailability after unsuccessful package install
- **System**
 - Fixed vulnerabilities CVE-2022-3524, CVE-2022-3566, CVE-2022-3567, CVE-2022-39188, CVE-2022-45934, CVE-2022-47929
 - Fixed bash vulnerability CVE-2022-3715
 - Fixed CGI-IO file download vulnerability CVE-2022-38333
 - Fixed libxml2 vulnerability CVE-2022-40304
 - Fixed libcurl vulnerabilities CVE-2022-43551 and CVE-2022-43552
 - Improved file upload logic
 - Fixed GPL firmware compilation with selected Tinc package
 - Fixed OpenVPN Static Key migration via keep settings issue
 - Fixed NTP time zone name setting migration when the name contains whitespaces
 - Fixed language setting issue
 - Fixed integer validation on industrial services
 - Fixed LED indications when PDP type is IPv6
 - Fixed issues with PDP type and SMS limit period migration via keep settings

[TCR1_R_00.07.03.4](#) | 2023.02.09

- **Fix**
 - **Network**
 - Changed generic modem restart method
 - Fixed mobile page VoLTE switching issues
 - **Services**
 - Sanitized tcpdump storage location
 - **System**
 - Fixed CVE-2023-32349 vulnerability

[TCR1_R_00.07.03.3](#) | 2023.01.25

- **Fix**
 - **Network**
 - Fixed disabled WiFi interface after factory reset

[TCR1_R_00.07.03.2](#) | 2023.01.13

- **New**
 - **System**
 - Japanese language
- **Improvements**
 - **Network**
 - Optimized mobile netifd script installation
- **Fix**
 - **Network**
 - Shortened modem hang monitor timeout
 - Fixed VLAN option setting when changing VLAN ID

[TCR1_R_00.07.03.1](#) | 2023.01.03

- **Improvements**
 - **System**
 - Remove front-end certificate validation
 - **Network**
 - Optimized mobile netifd script installation
- **Fix**
 - **Network**
 - Fixed modem communication validation
 - Fixed connection establishment in IPv6 only mode
 - **Services**
 - Fixed libxml2 vulnerability CVE-2022-40303
 - Fixed an IPsec Phase one & two setting migration issue
 - **System**
 - Fixed JSON key parsing; keys can now be any printable character sequence
 - Fixed memory leak in 'session' module
 - **WebUI**
 - Fixed file pretty name parsing

[TCR1_R_00.07.03](#) | 2022.12.16

- **New**
 - **Network**
 - Firewall DMZ page
 - **Services**
 - Java package
 - SFTP server support
 - OPC UA client
 - Hotspot registered users management page
 - **System**
 - Portuguese language
 - Spanish language
 - Turkish language
 - Email Relay package
 - **WebUI**
 - New Web menu design
- **Improvements**
 - **Network**
 - Updated modem handling, attachment, tracking and connection establishment processes
 - Added the possibility to select multiple ports in all firewall port fields
 - Added 'Match' traffic by type option to firewall traffic rules
 - Added DNS servers and routing table fields to the Wireguard page
 - Improved generating network topology
 - Moved Relayd, UDP Relay & Static Leases to the Interfaces menu section
 - Update Firewall Traffic Rules page with DSCP and MARK options
 - Added keepalive, holdtime and connect timers to BGP configuration
 - Added 'Use gateway metric' to network protocols web interface
 - Added more DHCPv6 client events to system log

- Moved IP Filter rules from Modbus TCP Gateway and Over IP services to Firewall page
- Added option to select subnet parameters in mobile Passthrough/Bridge modes
- Added WhereverSIM operator APN and fr.lebara.mobi APN to APN database
- Added mobile connection state for IPv6
- Added wget tracking method to WAN Failover
- Added interface checks to remove inaccurate Failover events from the Event Log
- **Services**
 - Added CSP headers to Hotspot Landing Page
 - Added hotspot user script validation
 - Improved logging of disconnecting client devices
 - Added execute custom script SMS Utilities rule
 - Added receiver and transceiver mode support to SMPP
 - Added timezone synchronization with GSM operator option to NTP Client
 - Updated Zerotier web interface
 - Added IPsec Flush connection option on tunnel initialization
 - Added MODBUS slave regfile validation
 - Added delay, number of timeouts, always reconnect options to MODBUS Master service
 - Added DMVPN Phase 2 and Phase 3 support
 - Added synchronization counting to NTP client
 - Expanded the data that is sent to the Cumulocity cloud with device log, mobile data usage and GPS data
 - Added 'Unregister' button to RMS page
 - Added new data monitoring options to SNMP: configuration state of wireless, smart queues & VLANs
 - Updated Zerotier package to version 1.10.1
 - Added automatic package removal upon failed installation in Package Manager
 - Added option to describe custom routing table and MTU auto counting to Wireguard VPN
 - Added IP blocking to MQTT Bridge for failed login attempts to prevent bruteforce attacks
 - Updated sqm-scripts to version 1.5.1
 - Improved MODBUS Master service: added multiple datatypes, added multiple register reading for alarms
 - Added monthly reboot option to periodic reboot function
 - Added support for multiple custom option selection to SSTP configuration
 - Added PKCS12 certificate chain support to OpenVPN
 - Improved MQTT to support multiple port listening, multiple bridge connections, notification settings and added support for custom configuration file
 - Added QoS selection to MQTT Modbus Gateway
 - Improved RAM usage during upload and installation of packages via Package Manager
 - Updated curl to version 7.86.0
 - Added brute-force prevention measures to Post/Get
 - Added automatic private and public key generation to Wireguard VPN
 - Added multiple Remote source IP support to IPsec
 - Added the possibility to configure multiple IPsec phase 1 and phase 2 proposals
 - Added functionality to rotate log file when log is saved to Flash memory
 - Improved performance while fetching packages on repeat visits to the Package Manager page

- **System**
 - Added a 'test mail' button to the Administration -> Recipients page
 - Added option to clear blocked IPs in the Access Control page after reboot
 - Updated Web Request-Response core logic
 - Added certificate validation to all services that support certificate upload
 - Updated URL protocol validations
 - Removed profile update requests during Save & apply
 - Optimized profile switching logic
- **WebUI**
 - Added an indication to the Interfaces page that displays when data limit is enabled
 - Added bootloader version to the Device section in the System page
 - Added configuration page shortcuts to Overview page widgets
 - Added tooltip in Overview that show free, used and total RAM/Flash values on mouse cursor hover
 - Updated network interfaces protocols web interface
 - Updated 404 page to include navigation menu
- **Fix**
 - **Network**
 - Fixed jumbo frames MTU issue
 - Added the 'Any' choice to source & destination IP address field in NAT rule edit
 - Fixed NHRP web interface issues
 - Fixed WAN interface configuration interfering with LAN
 - Fixed mdcollect memory leak issue
 - Fixed data limit not resetting properly
 - Fixed incorrect mobile data usage calculations for multiple day periods
 - Fixed an Auto APN 'Keep settings' issue
 - Fixed data counting after mobile data limit has been reached
 - Fixed mobile band not setting correctly on first try
 - Fixed incorrect data limit conditions causing unwanted SIM switches
 - Fixed Passthrough DHCP lease time setting
 - Fixed mobile bridge mode issue when no DNS servers are supplied
 - Added new Operator Lists instance name validations
 - Added individual WiFi toggle support
 - Added error message when DFS channel is selected during scanning
 - Fixed mac80211 vulnerabilities CVE-2022-41674, CVE-2022-42719, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722
 - Fixed wireless interfaces connections not reestablishing after disabling & enabling again
 - Updated DFS radar detection patterns for Japan
 - Fixed Wired WAN connectivity issue when Failover interfaces are disabled
 - Fixed Failover fallback issue
 - **Services**
 - Fixed an SMS rule Save and Apply issue
 - Fixed Hotspot connected user list maximum upload/download value limits
 - Fixed incorrect connected Hotspot user information in RMS JSON
 - Removed unnecessary field from the Port Mirroring page
 - Fixed Hotspot issues related to specific connected phones
 - Fixed Wireless AP enabled by MODBUS TCP Master not showing in Wireless clients
 - Fixed WiFi Scanner hostname validation issues

- Implemented Hotspot 'forget' method, which removes user from DB by MAC
- Fixed UCI SMS Rule return message to display new changes
- Fixed DNP3 issues when asking for modem temperature
- Fixed base64 encoding of SMS messages when forwarding to HTTP
- Fixed SMS sending issues when using multiple APN
- Added Gateway modem option to IP Block and WoL in SMS Rule edit
- Fixed unblocking IP addresses with an SMS message
- Fixed Mobile Utilities page not load properly on some occasions
- Fixed dbus vulnerability CVE-2020-35512
- Fixed dnsmasq vulnerability CVE-2022-0934
- Fixed ext4 vulnerability CVE-2021-3428
- Fixed kernel vulnerabilities CVE-2021-3669, CVE-2021-4203, CVE-2022-1353, CVE-2022-3435, CVE-2022-20008, CVE-2022-30594
- Fixed libxm12 vulnerability CVE-2022-29824
- Fixed Linux vulnerabilities CVE-2021-4148, CVE-2022-0480, CVE-2022-1055, CVE-2022-0886, CVE-2022-2663, CVE-2022-36879 for v5.4
- Fixed MQTT DoS vulnerability CVE-2021-41039
- Fixed privoxy vulnerability CVE-2021-44542
- Fixed python3 vulnerability CVE-2022-42919
- Fixed strongswan vulnerabilities CVE-2021-41991, CVE-2021-45079
- Fixed uboot vulnerabilities CVE-2022-30552, CVE-2022-30790
- Fixed CVE-2023-32350 vulnerability
- Fixed switching between RMS connection types while the device is unregistered
- Fixed reload issues in website blocking feature
- Fixed IPsec PSK secret required field validation
- Fixed bandwidth limiting after QoS is enabled for the first time
- Fixed Dropbear issues when logging in over IPv6
- Fixed Modbus status in Status -> Services page
- Fixed Azure IoT Hub application issues when sending large volumes of data
- Fixed Azure IoT Hub MQTT password validation
- Fixed DMVPN configuration migration issue
- Fixed DMVPN duplicate select options, added suffix to mobile interfaces to use IPv4
- Fixed DMVPN IPsec connection issue
- Fixed DMVPN mobile interface 'Keep settings' migration issue
- Fixed Dynamic DNS long hostname text display issue
- Fixed Events Reporting memory leak issue
- Fixed Events Reporting not triggering after flipping an I/O slider
- Fixed FOTA cron job not starting after factory reset
- Fixed IPsec local firewall option parsing
- Fixed IPsec tunnel creation issue when compatibility mode is used and the tunnel name contains an underscore
- Fixed L2TP, PPTP, SSTP state display in the Status -> Services page
- Fixed NTP pool hostname validation
- Fixed OpenVPN certificate remove with Static key and TLS authentication methods
- Fixed OpenVPN configuration saving issue when using HMAC key authentication
- Fixed OpenVPN custom dev name transformation to correct format
- Fixed OpenVPN device name setting logic when uploading config from file
- Fixed OpenVPN instance status display
- Fixed OpenVPN TAP (bridged) configuration detection

- Fixed Qos configuration saving issue occurring after instance deletion
- Fixed RMS JSON incorrect WAN state and IP information
- Fixed RMS step access issue in the Setup Wizard page
- Fixed SNMP issues after reboot while using a Hotspot
- Fixed SNMP generating MIB files for devices in accordance with to their hardware
- Fixed SNMP traps not working after SNMP is installed from server
- Fixed SSTP client route creation issue
- Fixed UPNP secure mode not turning off issue
- Fixed Wireguard route to endpoint issue
- Fixed manual package installation for queued packages
- Fixed NAT Rules dependency from IPsec web instance
- Returned usleep utility
- Updated Australian and South African NordVPN server IP addresses
- **System**
 - Fixed certificate signing issues
 - Fixed Telnet, CLI access blocking after max invalid tries
 - Fixed FW upgrade with 'Keep settings' while low free space is available
 - Fixed backup file duplication issue
 - Fixed network device handling in system
- **WebUI**
 - Fixed Hotspot interface display
 - Fixed side widget accessibility during first login
 - Fixed file upload issues
 - Fixed drag and drop issue in the Traffic Rules page
 - Fixed protocol display in the overview of the Interfaces page
 - Fixed blocked IP settings migration during a FW upgrade with the 'Keep settings'
 - Fixed login errors after browser tab restoration
 - Fixed redirect to newly set IP address after Interface configuration
 - Fixed firmware upgrade verify spinner not closing
 - Fixed an issue with file upload via drag and drop

[TCR1_R_00.07.02.7](#) | 2022.09.12

- **Improvements:**
 - Improved manual-auto connection mode
- **Fixes**
 - Fixed AT command for SMS storage usage
 - Fixed CVE-2022-1012 memory leak vulnerability
 - Fixed CVE-2022-37434 kernel vulnerability
 - Fixed interface option reset after VLAN ID change
 - Removed memory leak on port
 - Fixed WiFi Scanner out of range crash when iterating collected data

[TCR1_R_00.07.02.6](#) | 2022.08.24

- **Improvements:**
 - Added 'home.vodafone.de' APN
 - Improved stability of device information storage
- **Fixes:**
 - Added SMSC type omitting when empty SMSC number parsed in SMS PDU mode

- Fixed VoLTE management
- Fixed OpenVPN tls-auth and tls-crypt option names

TCR1_R_00.07.02.5 | 2022.08.12

- Improvements:
 - Updated curl to version 7.83.1
 - Updated firmware validation error messages
 - Added multiple source IP address support to the Port Forwards page
 - Increased custom APN Username & Password field maximum length to 64 symbols
 - Added auto switch to modem's SMS storage when SIM card storage doesn't exist
 - Improved mobile connection status handling
 - Added CSP headers Hotspot WebUI landing page
- Fixes:
 - Fixed CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208 curl vulnerabilities
 - Fixed CVE-2022-30065 busybox vulnerability
 - Fixed file upload path traversal
 - Removed Data to Server limit to process less than 10 instances
 - Fixed Data to Server 'out of memory' crashes when database is full or has a large amount of data
 - Fixed OpenVPN dev setting logic
 - Fixed OpenVPN updating from legacy issue that caused IPv6 not to work
 - Fixed MAC and leasetime setting for Bridge & Passthrough modes
 - Fixed modal tabs navigation when editing wireless interface with non-english languages
 - Fixed POST/GET output state being high after first request

TCR1_R_00.07.02.4 | 2022.07.20

- Improvements:
 - Added default password change warning message before firmware downgrade
 - Extended time period for device to make connection to operator
 - Reduced the number of modem reboots when changing mobile settings
 - Reduced excessive log output when no SIM card is inserted
 - Added modem restart prevention on modem init
 - Added disable RPLMN option in the SIM section of the SIM card config
- Fixes:
 - Fixed CVE-2022-2068 vulnerability
 - Disabled autoconnect on stop-network call
 - Fixed Hotspot login via landing page issue
 - Added firmware compatibility check

TCR1_R_00.07.02.2 | 2022.06.27

- Improvements:
 - Updated FSTools package to version 2022-05-03
 - Added security headers to web requests
 - Added ping to DNS IPv6 support
 - Added modem reset to default state after device FW upgrade
 - Modem init now checks NVRAM sensitive commands before setting
 - GSM output was made consistent

- Fixes:
 - Fixed CVE-2019-12900 libbz2 vulnerability
 - Fixed CVE-2022-23303 hostapd vulnerability
 - Fixed CVE-2022-29581 Linux kernel vulnerability
 - Fixed CVE-2022-29458 ncurses vulnerability
 - Fixed CVE-2022-1292 c_rehash script command injection vulnerability
 - Fixed behavior of some gsmctl commands
 - Fixed band locking issue
 - Fixed race condition for wireless configuration initialization

[TCR1_R_00.07.02.1](#) | 2022.06.06

- Improvements:
 - Improved GSM related messages in Troubleshoot logs
- Fixes:
 - Fixed default mobile network configuration generation
 - Fixed MODBUS write requests and Mobile Utils option setting

[TCR1_R_00.07.02](#) | 2022.05.23

- **New features**
 - Overview side widget
 - IGMP Proxy
 - Privileged Access Management (PAM)
 - AWS Greengrass support
 - HTTPS certificate and key upload feature
 - SSH public keys edit box
 - License page
 - DNP3 data for Data to Server
- **Improvements**
 - Updated busybox to version: 1.34.1
 - Updated curl to version 7.79.1
 - Added iptables filter package for string filtering
 - Added CHAP authentication for L2TP VPN
 - Added IPv6 support for L2TPv3 VPN
 - Added EAP-MSCHAPV2 authentication method for IPsec VPN
 - Added IPv6 support to Auto Reboot
 - Added 'Save to flash' and 'Test configuration' button to DNP3 configuration page
 - Updated SNMP version 5.9.1
 - Added OpenSSL authentication options to SNMPv3
 - Added support for OSPF redistribution options and OSPF neighbors
 - Added password field to BGP Peers page
 - Extended BGP "AS" field validation to accept integers up to 4294967295
 - Added "DHE+RSA" to OpenVPN cipher selections
 - Increased OpenVPN max password length from 128 bytes to 512 bytes
 - Made HMAC key direction initial value dependent on the role of the instance (client or server)
 - Made HMAC key and HMAC authentication key upload fields required
 - Added DES to IPsec encryption algorithms selections
 - Added special character support for CHAP secrets

- Added validation requirements for PPTP user list username field
- Added option to manually enter Public key in Wireguard configuration
- Made generating Wireguard keys possible only while in auto mode
- Added Events Log database to troubleshoot archive
- Added RFC1918 filter field
- Added the possibility to unblock multiple blocked devices at once
- Added 'Port' column to blocked login attempts table
- Added Speedtest server refresh
- Updated Speedtest server list
- Added asterisk option to Site Blocking
- Added MD5 and SHA256 checksums to package validation page
- Changed certificate requirements to only require client key file if client certificate is used
- Added pagination and data retention between table pages
- Added pagination functionality to tables when there are more than 10 records
- Improved table sorting by saving user provided sort settings in the browser
- Improved drag and drop functionality
- Added the possibility to drag and drop files onto upload components
- Moved 'Root CA' from the 'Access Control' page to the 'Certificates' page
- Added 'Strict-Transport-Security' response header for HTTPS
- Added 'breadcrumbs' to modal windows
- Improved initial WebUI loading after login
- Added mobile bytes sent and bytes received SNMP OIDs
- Added mobile LED turn off feature ('System -> Administration' page)
- Added 'iot.1nce.net', 'internet', 'VZWINTERNET' and Truphone APNs to APN database
- Updated mobile usage data point calculation logic
- Added the possibility to manually enter operator number
- Improved obtain mobile cell ID process
- Added modem restart if SIM card is removed during APN database fetching process
- Added unauthorized call logging
- Added space character support in SMS commands
- Disabled SMS modem storage configuration form when SIM is not inserted
- Changed SMS '%wi' parameter value to return IP address of any currently used WAN interface (not only wired)
- Added external modem SMS limit Overview card and widget
- Made in-use APNs visible next to mobile interface configurations (before clicking the 'Edit' button)
- Added duplicate value check for list configuration options
- Changed mobile card instance design
- Fixed 'Mobile Data usage reset' SMS rule
- Fixed the default state parameter of SMS list POST/GET command
- Added Hotspot configuration profiles
- Added local Hotspot user password hashing
- Added Hotspot password encoding option
- Improved Hotspot related firewall rule setting
- Improved WiFi Scanner enable switch to toggle 2 and 5 GHz instances separately
- Removed CHAP authentication protocol for WiFi Hotspots due to incompatibility with hashed passwords
- Added ubus support to Hotspot
- Changed default port name of WiFi devices for 'Topology state' Events Reporting rule
- Added I/O SNMP trap

- Added ISO 8601 time format to I/O Juggler's '%ts' parameter
- Added device name parameter '%pc' to I/O Juggler
- Added PPPoE VLAN priority support
- Made VRRP ping section dependent on main instance
- Added 'WAN to LAN' switch

- **Fixes**

- Fixed CVE-2021-20322, CVE-2021-4197, CVE-2022-1011, CVE-2022-0847 kernel vulnerabilities
- Fixed CVE-2022-28391 busybox vulnerability
- Fixed CVE-2018-16789 shellinabox vulnerability
- Fixed CVE-2021-44543, CVE-2021-44542 privoxy vulnerabilities
- Fixed CVE-2021-43618 GNU Multiple Precision Arithmetic Library vulnerability
- Fixed zlib backport security issue
- Fixed Wireguard firewall zone assignment
- Fixed queued packages disappearing from list after FW upgrade with keep settings
- Fixed error message display for multiple input validation rules
- Fixed incorrect DHCP validation range for start and limit fields
- Removed 'Bring up on boot' option from network interface configuration pages
- Fixed coma-separated DHCP options disappearing after save
- Fixed exclude and listen interfaces
- Fixed 'Use broadcast flag' option saving
- Fixed firewall zone assignment when creating new interfaces
- Fixed OpenVPN 'Netmask' and 'IP address' field validations
- Fixed OpenVPN TAP configuration saving issue
- Fixed OpenVPN switching to TUN mode when uploading a configuration from file
- Fixed dynamic BGP route state display
- Fixed BGP peer enable in edit page
- Fixed issue when no L2TP client instance could be bound to IPsec
- Fixed firewall rule and zone behavior related to config section creation
- Added default value for L2TPv3 netmask, which is now written to config after save
- Fixed passthrough option saving to IPsec file
- Fixed DMVPN issue where instance configuration could not be saved
- Fixed Wireguard peer could not be saved issue
- Fixed NTP client time synchronization after factory reset
- Fixed device time display with selected time zone
- Fixed MODBUS TCP indexation missing bracket issue
- SMS Utilities: enhanced service security
- Fixed initial MODBUS TCP request count validation
- Fixed PIN 3/4 direction switching over MODBUS TCP
- Fixed MODBUS data to MQTT socket closing issue when connection fails
- Fixed MODBUS alarm configuration deletion
- Fixed DNP3 master not working after FW upgrade with 'keep settings'
- Fixed DNP outstation not returning error messages
- Added missing SNMP objects: mobile IP, data sent/received today
- Fixed MQTT Publisher 'Remote address' field validation
- Fixed long interface name support for Azure IoT Hub
- Increased maximum Azure IoT Hub 'Connection String' length to 4096 characters
- Fixed missing sent/received data issue
- Fixed URL input field length validation
- Fixed admin login issue after upload of backup from a device with older firmware

versions

- Fixed MAC address formatting in Events reporting messages
- Fixed Events reporting DHCP lease message spam, when no new lease is added
- Fixed logging crashing after downloading Troubleshoot file
- Made Wake on LAN visible only on devices with Ethernet ports
- Fixed Traffic log file transfer to FTP server
- Fixed Web Filter service reloading after a host list file is uploaded
- Fixed access denied messages when sending JSON-RPC requests from root user
- Fixed error message display about duplicated intervals in Profile scheduler
- Fixed FW upgrade with 'keep settings' migration issue for Access Control's 'Fail count' and 'Device port' fields
- Corrected OSPF Routing card values, value positions and names
- Fixed global secret instances not being removed when there are no IPsec instances
- Fixed uploaded file remove icon not staying in position on hover
- Fixed Overview card collapse issue that made it unresponsive after too many clicks
- Removed WAN6 interface from the Overview page
- Fixed mobile IPv6 display in Events Reporting status messages
- Fixed Bridge mode when DNS2 is not available
- Fixed PAP/CHAP username and password fields not saving in interface edit window
- Fixed sending email without secure connection for providers that support such an option
- Fixed 'N/A' parameter showing up in SMS Utilities monitoring status message
- Fixed Call Utilities Events Log message for reboot rule
- Fixed SMS command validation for no-authorization option
- Fixed MODBUS SMS alarms 'Enable' option saving
- Fixed running RMS with no SIM card inserted issue
- Fixed firmware available on server version checking issue
- Fixed CVE-2020-15078 openvpn vulnerability
- Fixed storage calculation for packages
- SMS Utilities: enhanced service security
- Fixed firmware deletion after leaving the page
- Fixed setup wizard redirect after LAN IP change
- Fixed various validation bugs, typos, option hints & alignments
- Fixed multiple IPv6 configuration field validations
- Added multiwan support for Wireguard default route
- Fixed wireless signal strength display when no clients are connected
- Fixed loss of connectivity for clients when router is in STA+AP mode
- Added validation that prevents automatic connection to first unencrypted WiFi AP when using MULTI AP
- Fixed Wifi Scanner data not being stored in certain scenarios
- Fixed WiFi scanner not turning on after FW upgrade with 'keep settings'
- Fixed Hotspot user group limit not resetting on specified time
- Removed an RMS error message when no Hotspot users were created
- Fixed Hotspot landing page image upload issue
- Fixed issue that prevents saving Guest Network configuration changes

TCR1_R_00.07.01.4 | 2022.02.25

Note: Firmware version TCR1_R_00.07.01.4 released on 2022.02.25 was removed due to an issue with improper firmware validation.

• Improvements

- Increased Port Forwards rule max name length

- **Fixes**

- Added missing bracket to the end of MODBUS messages
- Fixed preserving the contents of /etc/luci-uploads/ after FW upgrade with the 'Keep all settings' option
- Fixed IPv4-Gateway column showing empty values in the Status -> Routes page
- Fixed firewall extra option validation
- Fixed Hotspot enable button validation
- Removed invalid network interface selections from the "Network" dropdown in the Wireless interface configuration page
- Changed the logic of uploading files to the modem
- Fixed OpenVPN server configuration with password authentication
- Fixed NTP interval length validation
- Fixed network interface enable after Drag & Drop
- Updated NTP client interval to 24h
- Fixed connection to whitelist carriers
- Fixed Passthrough mode when DHCP is disabled
- Fixed 'Deny data roaming' feature
- Fixed mobile blocking dependency on region
- Disabled Ping To DNS functionality when Bridge/Passthrough mode is enabled

TCR1_R_00.07.01.2 | 2022.01.04

Note: Firmware version TCR1_R_00.07.01.2 released on 2022.01.04 was removed due to an issue with improper firmware validation.

- **New features**

- DFOTA modem upgrade system for Quectel modems

- **Improvements**

- Removed L2TP section title prefixes

- **Fixes**

- Fixed IPSec crashing issue using mobile
- Fixed FW flashing when chip is in unknown state
- Fixed CPU usage percentage display in the Overview page
- Fixed FOTA timeout issue when server does not respond
- Fixed installation of backup packages
- Fixed mobile data limit display after profile change
- Fixed Bridge mode without multi-APN
- Fixed multi mobile interface checking
- Fixed error handling when the modem is not responding
- Prolonged autoconnect setting timeout

TCR1_R_00.07.01 | 2021.11.18

Note: Firmware version RUTX_R_00.07.01 released on 2021.11.18 was removed due to an issue with IPsec tunnel while using mobile connection.

- **New features**

- Initial TCR100 Firmware