

RUT300 Firmware Downloads

[Main Page](#) > [RUT Routers](#) > [RUT300](#) > **RUT300 Firmware Downloads**

This page contains firmware files for RUT300 devices. Look to the table below or the [changelog](#) to find download links.

To upgrade firmware using WebUI, follow the instructions in [RUT300 Firmware](#).

RUT300

File	Type	Release date	Size	MD5	Changelog
RUT30X_R_00.07.06.10_WEBUI.bin	Latest FW	2024.04.04	10.13 MB	1c7a2958289eb77b9c66983757f114b7	Link
RUT30X_R_00.07.06.5_WEBUI.bin	Mass production FW	2024.02.21	10.44 MB	11dfbb85cd4af4a35f3e56229b2eef95	Link
RUT30X_R_GPL_00.07.06.10.tar.gz	SDK	2024.04.04	19.23 MB	237110a8ab99f8ed8f8675e6c5ab20d6	

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

Global RUTOS changelog can be found here: [LINK](#)

* This is universal changelog of RUTOS. Changes made to features that are not present in some devices, do not affect them.

[RUT30X_R_00.07.06.10](#) | 2024.04.04

- Global changelog for **R_00.07.06.10** - [LINK](#)

[RUT30X_R_00.07.06.8](#) | 2024.03.25

- Firmware **R_00.07.06.8** was removed due to an issue with inefficient memory allocation for LED control.

[RUT30X_R_00.07.06.6](#) | 2024.03.04

- Global changelog for **R_00.07.06.6** - [LINK](#)

[RUT30X_R_00.07.06.5](#) | 2024.02.21

- Global changelog for **R_00.07.06.5** - [LINK](#)

[RUT30X_R_00.07.06.3](#) | 2024.01.17

- Global changelog for **R_00.07.06.3** - [LINK](#)

[RUT30X_R_00.07.06.1](#) | 2024.01.04

- **Fix**
 - **Services**
 - Fixed issue with NTPclient zombie processes

[RUT30X_R_00.07.06](#) | 2023.12.20

- **New**
 - **Services**
 - Added OPC UA Server
 - Added the ability to set port for TACACS+ in PAM service
 - Added switch to enable using root certificate authority for MQTT alarms in Modbus Client services
 - Added new alarm action "Ubus event" in Modbus Client services
 - Added new input "Modbus alarms" in Data to Server service
 - Added wget ping subtype support in Events Reporting service
 - Added new I/O SNMP OID that returns numeric I/O state
 - Added TLS support for OverIP serial functionality
 - **WebUI**
 - Renewed user interface design
 - Added network interface name change functionality
 - Added last resort configuration option for multiwan policy rules
 - **System**
 - Added ability to enable/disable SSH access for specific users in System Users
 - API support
- **Improvements**
 - **Services**
 - Expanded GRE VPN keep alive functionality to disable routes from unreachable tunnel
 - Added PKCS#12 certificate container authentication method in IPsec VPN
 - Added TLV message_payload support for SNMP service
 - Added Purple.ai configuration profile
 - Replaced option "No leading zeros" with "Remove all zeros" in Over IP serial

- functionality
 - Added reboot on storage device disappearance and re-appearance
- **WebUI**
 - Improved Events Log page loading by adding asynchronous pagination
 - Removed requirement for Diffie-Hellman parameters in OpenVPN service
 - Added improvements for creating OpenVPN IPv6 configurations
 - Added auto redirect after changing router's IP address or port
 - Added "Interface" dropdown for interfaces selection in Wake on LAN service
 - Increased Data to Server service MQTT topic length limit to 65535 characters
 - Added OSPF external routes section to Status page
 - Moved device menu entry "Reboot" to header menu
- **System**
 - Added Mosquitto CVE patch 2023-28366
 - Added Mosquitto CVE patch 2023-3592
 - Updated cURL version to 8.4.0
 - Updated kernel version to 5.4.259
 - Added RMS data display to generated troubleshoot
 - Added downloaded Package Manager packages list to generated troubleshoot
 - Added process activity load list to generated troubleshoot
 - Changed default OPKG feed to use Teltonika's URL
- **Fix**
 - **Network**
 - Fixed DMVPN firewall rule creation issues
 - Fixed Failover missing active rules when using multiple source and destination IP addresses
 - **Services**
 - Fixed SSH module enable in PAM service
 - Added minimum free space check when saving logs to flash in Logging service
 - Fixed "Set multiple coils" function sending too many bytes in Modbus Client services
 - Fixed multiple Events Reporting messages being sent when Firewall configuration is changed
 - Fixed VRRP instances advertising wrong virtual IPs
 - Added Hotspot information in SNMP MIB file
 - Fixed registered Hotspot Local Users showing random username
 - Fixed selection of MAC Auth for LAN interfaces in Hotspot service
 - Fixed inconsistent Hotspot login behaviour when using MAC Auth with Password
 - Fixed instance shutdown after last local user deletion
 - Fixed RMS Hotspot data display for devices without WiFi support
 - Fixed serial timeout not working in Over IP serial functionality
 - Removed "Echo" option in Modbus TCP over Serial functionality
 - Fixed CRC verification failing when CRC is correct in Modbus TCP over Serial functionality
 - Fixed crash when getting unexpected messages from RTU in Modbus TCP over Serial functionality
 - **WebUI**
 - Fixed side menu style issues when Japanese language is used
 - Fixed displaying of vendor names in Topology page
 - Fixed language packs being selectable when still in Package Manager queue
 - Added ability to configure IPv6 BGP peer

- Fixed realtime graphs responsive design issues
- Fixed Network Shares users deletion
- Fixed not all LAN interfaces shown in dropdown in Hotspot service page
- **System**
 - Patched FRR CVE-2023-38406
 - Patched FRR CVE-2023-38407
 - Patched FRR CVE-2023-41358
 - Patched FRR CVE-2023-41360
 - Patched FRR CVE-2023-41909
 - Patched FRR CVE-2023-47234
 - Patched FRR CVE-2023-47235
 - Patched OpenSSL CVE-2023-3446
 - Patched OpenSSL CVE-2023-3817
 - Patched LibXML2 CVE-2023-39615
 - Patched LibXML2 CVE-2023-45322
 - Patched FFMPEG CVE-2021-28429
 - Patched FFMPEG CVE-2022-48434
 - Patched dnsmasq CVE-2023-28450
 - Fixed running out of space when SSHFS is mounted in /tmp while generating troubleshoot

[RUT30X_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

[RUT30X_R_00.07.05](#) | 2023.10.09

- **New**
 - **Network**
 - Software Offloading enabled on default configuration
 - **Services**
 - DLMS Client package
 - 7zip package
 - TincVPN package
 - Added router uptime parameter 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
 - Speed Test package
 - **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
- New "Server+Client" work mode in OverIP Serial Utility
- New "Connect on data" action in OverIP Serial Utility
- Multiple Client instance support in OverIP Serial Utility
- IPv6 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
 - **Services**
 - Added Modbus Serial functionality
 - 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
 - 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
- Removed redundant "Action" option in Periodic Reboot
- Added IPv6 support in OverIP serial utility
- **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 curl version to 7.88.0
 - 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 wrong or empty WAN state info
- 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 data being lost when sending large packets to serial devices using OverIP serial utility
- Fixed OverIP possible serial device overflow and minor bugs
- More robust error recovery for RTU communication in Modbus Client service
- Fixed user deletion in Network Shares service

- Fixed router reboot inconsistencies after Storage Memory Expansion
- **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 disabling DLNA service when USB drive is removed
- **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-2023-36369 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
 - Fixed backup upload validation with memory expansion

[RUT30X_R_00.07.04.5](#) | 2023.07.24

- **Improvements**
 - **Network**
 - Added metric field support in BGP Route-maps page

[RUT30X_R_00.07.04.4](#) | 2023.06.26

- **Improvements**
 - **Services**
 - Improved UPNP lease file validation
 - Improved DLNA 'Database directory' field validation to not allow ', ` and spaces
 - **System**
 - Device name is now displayed in browser tab when in login page

- **Fix**
 - **Network**
 - Patched CVE-2023-32233 vulnerability
 - Fixed default networks in WAN firewall zone and possibility to add 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

[RUT30X_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**
 - **System**
 - Fixed an issue on bootloader web recovery hanging with certain firmware sizes

[RUT30X_R_00.07.04.2](#) | 2023.04.18

- **New**
 - nftables support
- **Improvement**
 - **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 libiwininfo to version 2022-08-19
- **Fix**
 - **Network**
 - Fixed Port-based VLAN ID calculation issue
 - **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 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

[RUT30X_R_00.07.04.1](#) | 2023.03.24

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

[RUT30X_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
 - **Services**
 - Added MQTT support to I/O Juggler
 - 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
 - Improved error messages in the Serial Utilities page
 - **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
- **Fix**
 - **WebUI**
 - Fixed Services page not displaying data after Thingworx package is installed
 - Added DNP3 to the 'Status > Services' page
 - **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
- **Services**
 - Fixed the listing of slow USB devices such as HDDs
 - Fixed DNP3 serial master not working when Stop bits are set to 2
 - Fixed DNP3 requests not deleting along with instance
 - Fixed DNP3 memory leak occurring after spamming the test request button
 - Fixed Serial Over IP related Firewall rule setting
 - 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 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

[RUT30X_R_00.07.03.4](#) | 2023.02.09

- **Fix**
 - **Network**
 - Fixed CVE-2023-32349 vulnerability
 - **Services**
 - Sanitized tcpdump storage location

[RUT30X_R_00.07.03.2](#) | 2023.01.13

- **New**
 - **System**
 - Japanese language
- **Fix**
 - **Network**
 - Fixed VLAN option setting when changing VLAN ID

[RUT30X_R_00.07.03.1](#) | 2023.01.03

- **Improvements**
 - **System**
 - Remove front-end certificate validation
- **Fix**
 - **Services**
 - Fixed libxml2 vulnerability CVE-2022-40303
 - Fixed an IPsec Phase one & two setting migration issue
 - Returned missing udp_client_count option to Over IP mode
 - **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

[RUT30X_R_00.07.03](#) | 2022.12.16

- **New**
 - **Network**
 - Firewall DMZ page
 - **Services**
 - Java package
 - SFTP server support
 - OPC UA client
 - Hotspot 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 wget tracking method to WAN Failover
 - Added interface checks to remove inaccurate Failover events from the Event Log
 - **Services**
 - Added format button for each USB device in USB Tools General page
 - Reduced waiting time during storage device setup for Memory Expansion
 - Optimized Storage Memory Expansion package size
 - Replaced ntfs-3g with kernel-mode driver
 - Added USB to Serial support for Modbus, MQTT Modbus Gateway, NTRIP, DNP3
 - 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 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 CVE-2023-32350 vulnerability
 - 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 Wired WAN connectivity issue when Failover interfaces are disabled
 - Fixed Failover fallback issue
 - **Services**
 - Fixed Printer service starting issue
 - Fixed Printer service boot issues
 - Fixed DLNA service reload issues on USB drive insert/remove
 - Fixed relay state switching
 - Fixed Save & Apply issue with ADC/ACL type condition on I/O Juggler
 - Added I/O restart on configuration profile change
 - Fixed I/O voltage range display for power socket pins
 - Fixed SMNP OID for I/O state
 - Removed unnecessary field from the Port Mirroring page
 - 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 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 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

[RUT30X_R_00.07.02.7](#) | 2022.09.12

- **Fixes**
 - 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 events
 - Fixed WiFi Scanner out of range crash when iterating collected data

[RUT30X_R_00.07.02.6](#) | 2022.08.24

- **Fixes:**
 - Fixed OpenVPN tls-auth and tls-crypt option names

[RUT30X_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
- 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

RUT30X_R_00.07.02.4 | 2022.07.20

- Improvements:
 - Added default password change warning message before firmware downgrade
- Fixes:
 - Fixed CVE-2022-2068 vulnerability
 - Fixed Hotspot login via landing page issue

RUT30X_R_00.07.02.2 | 2022.06.27

- Improvements:
 - Updated FSTools package to version 2022-05-03
 - Added security headers to web requests
- 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 race condition for wireless configuration initialization

RUT30X_R_00.07.02.1 | 2022.06.06

- Fixes:
 - Fixed IGMP Proxy menu item not appearing after package installation
 - Fixed MODBUS write requests

RUT30X_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 error code 5 for reserved SAMBA user names
- Added Mobile data and SMS limit features for external modem
- 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** Added multiwan support for Wireguard default route
- 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
- 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 Cumulocity connection issue

- Hidden phone groups menu
- Fixed I/O Juggler external modem recognition
- Fixed flash driver reformatting after memory shrink
- Fixed DLNA package installation issue
- Changed Media Directories field to be required
- Fixed SAMBA fields value display
- Fixed relay output value display in I/O Juggler condition page
- Fixed I/O Juggler's WiFi rule not enabling or disabling WiFi interfaces
- Fixed I/O Juggler's double delete issue on I/O Juggler action and condition instances
- Fixed I/O Juggler's incorrect I/O status messages
- Fixed Wake On LAN issue

[RUT30X_R_00.07.01.4](#) | 2022.02.25

• Fixes

- 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

[RUT30X_R_00.07.01.3](#) | 2022.02.15

• Improvements

- DFOTA modem upgrade system for Quectel modems

• 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

[RUT30X_R_00.07.01.2](#) | 2022.01.04

• Improvements

- DFOTA modem upgrade system for Quectel modems

• 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

RUT30X_R_00.07.01 | 2021.11.18

Note: Firmware version RUT30X_R_00.07.01 released on 2021.11.18 was removed due to an issue with IPsec tunnel while using mobile connection.

• New features

- Load Balancing Rules

- Tinc VPN
- German language support

- **Improvements**

- Improved WebUI functionality when multiple browser tabs are open
- Updated base to OpenWrt version 21.02
- Updated kernel to version 5.4.141
- Updated mtd-utils to version 2.1.2
- Updated busybox to version 1.33.1
- Updated ubus to version 2021-06-3
- Updated ubox to version 2020-10-25
- Updated rpcd to version 2021-03-11
- Updated opkg to version 2021-06-13
- Updated fstools to version 2021-01-04
- Updated wwan to version 2019-04-29
- Updated ethtool to version 5.10
- Updated uhttpd to version 2021-03-21
- Updated ppp to version 2020-10-03
- Updated odhcpd to version 2021-07-18
- Updated hostapd to version 2020-06-08
- Updated dropbear to version 2020.81
- Updated dnsmasq to version 2.85
- Updated netifd to version 2021-07-26
- Updated firewall3 to version 2021-03-23
- Updated libjson-c to version 0.15
- Updated libevent2 to version 2.1.12
- Updated mac80211 to version 5.10.42-1
- Updated wireless-regdb to version 2021.04.21
- Updated binutils to version 2.35.1
- Updated gdb to version 10.1
- Updated strace to version 5.10
- Updated trace-cmd to version 2.9.1
- Updated valgrind to version 3.16.1
- Updated ath10k-ct-firmware to version 2020-11-08
- Updated procd to version 2021-02-23
- Updated iw to version 5.9.8
- Updated iproute2 to version 5.11.0
- Updated iptables to version 1.8.7
- Updated nettle to version 3.6
- Updated libpcap to version 1.9.1 rel3
- Updated elfutils to version 0.180
- Updated cryptodev-linux to version 1.11
- Updated linux-firmware to version 20210118
- Updated util-linux to version 2.36.1
- Updated openwrt-keyring to version 2021-02-20
- Updated mtd to version rel26
- Updated fwtool to version 2019-11-12
- Updated ca-certificates to version 20210119
- Updated wireguard-tools to version 1.0.20210223
- Updated iwinfo to version 2021-04-30
- Updated ipset to version 7.6

- Updated gre to version rel12
- Updated wolfssl to version 4.7.0
- Updated ustream-ssl to version 2020-12-10
- Updated uclient to version 2021-05-14
- Updated readline to version 8.1
- Updated mbedtls to version 2.16.11
- Updated libusb to version 1.0.24
- Updated libunwind to version 1.5.0
- Updated libubox to version 2021-05-16
- Updated libnl-tiny to version 2020-08-05
- Updated libnftnl to version 1.1.8
- Updated libiconf-full to version 1.16
- Updated libbsd to version 0.10.0
- Updated gmp to version 6.2.1
- Updated ulogd to version rel6
- Updated sqm-scripts to version 1.5.0
- Updated ntpclient to version rel14
- Updated nmap to version 7.80
- Updated curl to version 7.77.0
- Updated zerotier to version 1.6.5
- Updated xtables-addons to version 3.13
- Updated xl2tpd to version 1.3.16
- Updated stunnel to version 5.59
- Updated strongswan to version 1.0.13
- Updated sstp-client to version 1.0.13
- Updated pptpd to version rel5
- Updated openvpn to version 2.5.3 rel2
- Updated ntpd to version rel3
- Updated net-snmp to version rel2
- Updated mosquitto to version 2.0.11
- Updated miniupnpd to version 2.2.1 rel 3
- Updated etherwake to version rel5
- Updated libzip to version 1.7.3
- Updated libpgp-error to version 1.39
- Updated glib2 to version 2.66.4
- Updated libnetfilter-conntrack to version 1.0.8
- Updated libnetfilter-log to version rel3
- Updated lzo to version rel4
- Updated nghttp2 to version 1.43.0
- Updated openvpn-easy-rsa to version 3.0.8 rel3
- Updated iperf to version rel2
- Updated iperf3 to version 3.10.1
- Updated e2fsprogs to version 1.45.6
- Updated fuse to version 2.9.9
- Updated udprelay to version 2020-02-26
- Updated qmicli to version 1.28.2
- Updated pcre to version 8.45
- Updated libsmpp34 to version 1.14.1
- Updated libiwinfo to version 2.1
- Added netifd library for additional information related to network interfaces
- Updated openssl to version 1.1.1l

- Updated privoxy to version 3.0.32
- Added ACL reload method for sessions
- Added 'Advertisement interval' field to the VRRP configuration window
- Added a PPTP-to-WAN Zone Forwarding rule when default route is enabled on PPTP client
- Added email user group validation for sending test emails with Events reporting
- Added an event logging feature for Ping Reboot events
- Improved file/section deletion logic: now files are also deleted after deleting a related config section
- Improved package deletion logic
- Added the possibility to configure multiple reboot times in one Reboot Scheduler configuration instance
- Updated 'External system log server' field validation to accept IPv6 addresses
- Added redirect to Overview page after login
- Added WebUI session timeout after user inactivity
- Added placeholder text to dropdown menus
- Improved multi-select design and functionality
- Added Unix timestamp, local ISO time, UTC time to Modbus
- Added info message when selected file cannot be uploaded
- Improved IPsec throughput
- Added IPsec "Compatibility mode" configuration support
- Made SNMP 'Community name' option editable
- Added new configuration options to the Failover feature
- Changed Failover page availability from Advanced only both advanced and basic
- Made Failover Interfaces table rows draggable when in 'Load Balancing' mode
- Changed Failover page 'Ratio' fields to a smaller size
- Added external modem support for the 'Mobile Usage' graph
- Added I/O support to SNMP
- Removed ubus list method due to security reasons
- Added MODBUS "%I, %T, %S, %r, %n" support to MODBUS Data Sender
- Removed search engine site crawling
- Improved IPsec "Local/Remote source" validation
- Added Firewall "all" and "custom" protocol options
- Added Backup file size limit of 2 MB
- Improved basic/advanced mode changing
- Improved Wireguard "IP Addresses" field validation
- Added language download support from language selection section
- Added PPTP "Client to client" configuration support
- Made DDNS "username", "password", "host" fields optional
- Added SSTP "Default route" configuration support
- Added I/O action support MODBUS Alarms
- Added "Topology state" support to Events Reporting

• Fixes

- Made RMS 'Connect' button disabled when a connection attempt is already in progress
- Added validation for TLS Clients 'Private network' option
- Fixed the validation range for MTU fields
- Fixed removing firmware image file after leaving the firmware upgrade page
- Fixed network selection list for Traffic Logging - added all available LAN networks
- Fixed DHCP Options validation
- Fixed configuration profile date display

- Fixed blank page after invalid URL in login page
- Fixed TR-069 related firewall rule loading
- Fixed remote subnet netmask validation issues for the GRE Tunnel configuration
- Fixed WebUI section toggle
- Fixed package installation modal layout
- Fixed current page values showing up in login page username field
- Fixed the possibility to create section with a name that is already in use in the same config file
- Fixed OpenVPN username and password deletion when deleting configuration instance
- Fixed session closing issue for the user whose password was just changed
- Updated MODBUS credential validation
- Updated MQTT credential validation
- Fixed DNS 'Rebind protection' setting when switch is disabled
- Updated libgcrypt to version 1.9.3 to fix CVE-2021-33560
- Fixed CVE-2021-33624, CVE-2021-29648 vulnerabilities
- Fixed DHCP 'Lease time' and 'Unit' option saving over the Setup Wizard LAN page
- Fixed Reboot Scheduler not removing crontab file after disabling the rule
- Fixed OpenVPN 'Extra options' field validation to allow a space character
- Added table drag and drop functionality to the Firewall's Traffic Rules page
- Fixed DNP3 Outstation crash caused by non-void function returning no value
- Fixed RMS 'Copy' button functionality
- Fixed incorrect loading after saving Failover configuration
- Fixed I/O Juggler hour condition interval issue
- Patched CVE-2021-40528 vulnerability
- Patched CVE-2021-40490 vulnerability
- Patched CVE-2020-16120 vulnerability
- Fixed VLAN section creation
- Returned Interfaces "Port priority" option
- Fixed missing Content-Type header to initial WebUI response
- Fixed RIP information parsing in status page
- Fixed OpenVPN IPv6 netmask validation
- Fixed SNMP Trap Settings Host/IP field validation
- Fixed Cumulocity authentication reset
- Fixed Events Reporting rule saving

RUT30X_R_00.07.00 | 2021.07.16

• New features

- New WebUI based on Vue.js 2.6.12
- RutOS updated to OpenWrt 19.07.7 base
- DNP3 Master and DNP3 Outstation

• Improvements

- Updated firewall to release 3
- Updated kernel to version 4.14.221
- Updated uhttpd to version 2020-10-01
- Updated xtables-addons to release 9
- Updated mwan to version 2.8.14
- Updated pcre to version 8.44
- Updated curl to version 7.74
- Updated sqlite to version 3.33
- Updated ncurses to version 6.2

- Updated OpenSSL to version 1.1.1k
- Added full MODBUS register address expansion specifier for Data to Server
- Added full MODBUS register address legend
- Added Client ID option for the MQTT protocol in Data to Server
- Improved Data to Server sleeping accuracy
- Improved Data to Server username validation; now space is allowed
- Added firmware version OID to the SNMP service
- Added IP address family option field to the SNMP page
- Added SNMPv6 section to the SNMP Communities page
- Renamed the 'System -> Users' page to 'System -> System Users'
- Moved password changing option to the 'System -> System Users' page
- Switched to ar8216 driver
- Added IPsec XAUTH support
- Improved OpenVPN updown, init scripts to write info about instance in JSON
- Added AES-256-GCM encryption support to OpenVPN
- Added extra configuration parameters to DMVPN
- Added PSK conversion to DMVPN and single PSK types
- Improved Package Manager package installation, deletion and dependencies
- Improved Package Manager download process over FOTA
- Added new Input/Output values manageable over RMS
- Added IPv6 traffic logging
- Made 'Network -> Failover' and 'Network -> Interfaces' page data draggable on multiple browsers
- Added Input/Output Post/Get URL parameter t_time changing delay and time to seconds or milliseconds
- Added support for multiple USB to Serial adapters
- Added peer groups to BGP access list dropdown
- Added TCP MD5 authentication support for BGP

• Fixes

- Added glib2 patch to fix CVE-2019-13012 vulnerability
- Added ntfs-3g patch to fix CVE-2019-9755 vulnerability
- Added WolfSSL patch to fix CVE-2021-3336 vulnerability
- Added Busybox patch to fix CVE-2018-1000500 vulnerability
- Added netifd, odhcp6c IPv6 routing loop on point-to-point links patches to fix CVE-2021-22161 vulnerability
- Fixed Android clients IPsec MTU/MSS size
- Fixed wrong IPsec DPD value saving
- Changed IPsec PSK maximum length to 128 symbols
- Fixed SSTP remaining up after package removal
- Fixed DMVPN crypto_proposal write to config
- Fixed I/O Juggler's SMS sending to correct group
- Fixed I/O Scheduler's relay state issue
- Added I/O direction check while changing IOs via I/O Post/Get
- Fixed float endianness mismatch on some devices MODBUS TCP Master, MODBUS Serial Master
- Fixed UPnP issue that caused config changes to apply only after service restart
- Fixed WebUI files caching when upgrading firmware
- Fixed WebUI date display format
- Fixed MODBUS returning incomplete MAC address data
- Fixed 'Over IP' serial type's UDP issue in client mode

- Fixed DLNA connections count total in statistics page

RUT30X_R_00.02.06.1 | 2021.02.10

- **Fixes**

- Added dnsmasq patch CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687
- Fixed PPTP server interface naming
- Fixed correct client PPTP interface name selection for route creation
- Fixed adding helper to firewall's wan zone when enabling PPTP configuration
- Added package size checking when manually installing a package
- Fixed 'New Firmware Available' message display after firmware upgrade

RUT30X_R_00.02.06 | 2020.12.31

- **New features**

- Initial RUT300 Firmware