DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

Digi TX/LR Firmware Release Notes
Version 22.5.50.62 (June 2022)

INTRODUCTION

Digi Accelerated Linux is an advanced, high-performance operating system for cellular routers. These are the release notes for the initial Digi Accelerated Linux (DAL) firmware release, which supports the Digi TX and LR family of products listed below.

SUPPORTED PRODUCTS

- Digi TX54
- Digi TX54 Primary Responder
- Digi TX64
- Digi TX64 Primary Responder
- Digi TX64 Rail
- Digi TX64 Rail Primary Responder
- Digi LR54

KNOWN ISSUES

- The Serial status and statistics for the TX54 are incorrect on the Web UI and CLI. [DAL-5763]
- Health metrics are uploaded to Digi Remote Manager unless the **Monitoring > Device Health > Enable** option is de-selected and either the **Central Management > Enable** option is de-selected or the **Central Management > Service** option is set to something other than Digi Remote Manager. [DAL-3291]

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you deploy production devices.
2. Unless otherwise noted, apply updates in the following order:
    a. Device firmware
    b. Modem firmware
    c. Configuration
    d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, see the Digi Remote Manager User Guide.

If you prefer manually updating one device at a time, follow these steps:

1. Download the **22.5.50.62** firmware update image from the Digi support website to your PC
    - TX54
        - TX54-Single-Cellular-22.5.50.62.bin
        - TX54-Dual-Cellular-22.5.50.62.bin
        - TX54-Dual-Wi-Fi-22.5.50.62.bin
    - TX64
        - TX64-22.5.50.62.bin
    - TX64 Rail
        - TX64-Rail-Single-Cellular-22.5.50.62.bin
    - TX54 Primary Responder
    - TX64 Primary Responder
    - TX64 Rail Primary Responder
        - Please contact tech.support@digi.com for the firmware update files.
    - LR54
        - LR54-22.5.50.62.bin
        - LR54W-22.5.50.62.bin

2. Log into the Web UI.
3. Navigate to the **System > Firmware Update** page.
4. Click **Choose File** and select the appropriate firmware update image.
5. Click **UPDATE FIRMWARE**.
6. The device will automatically reboot once the firmware update is complete.

Upgrading from releases prior to release 22.2.9.85

If you are upgrading your TX64 device by using the local Web UI, you must first upgrade to release 22.2.9.85 prior to upgrading to the current release.

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, knowledgebase, and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

Mandatory release - A firmware release with a critical or high security fix rated by CVSS score.

For devices complying with ERC/CIP and PCIDSS, their guidance states that updates are to be deployed onto devices within 30 days of release

Recommended release - A firmware release with medium or lower security fixes or no security fixes

Note that while Digi categorizes firmware releases as mandatory or recommended, the decision on when to apply the firmware update must be made by the customer after appropriate review and validation.

VERSION 22.5.50.62 (June 2022)

This is a **mandatory** release.

NEW FEATURES

1. WAN bonding support for bonding multiple WAN connections together for increased maximum throughout or redundancy has been added to the TX54 and TX64 platforms.

   Note: This support can only be enabled using Digi Remote Manager.
2. A Serial PPP dial-in mode for handling AT based connection requests from a device connected on a serial port and providing IPv4 networking to the device.

ENHANCEMENTS

1. The SCEP client support has been enhanced to work with a wider range of SCEP servers.

   The following SCEP servers have been tested:
   - Fortinet FortiAuthenticator
   - DigiCert
   - EJBCA
   - Windows Server

   A new **show scep** CLI command has been added to display the status of the configured SCEP clients.
2. The Wi-FI Scanner functionality has been updated to allow the Wi-Fi Scanner results to be pushed to one or more remote servers using a TCP or HTTP connections.
3. The SureLink “Reset Modem” action has been enabled by default on cellular interfaces with the fail count set to 3. The modem will be automatically power cycled in the event the modem fails to reset correctly.
4. 5G slicing support for a single slice has been added to the TX64 5G platforms.
5. The location support has been updated to support different NMEA sentence content options when forwarding the NMEA sentences to a remote server and there is no valid fix.
6. The cellular APN and connection time have been added to the data points that are uploaded to Digi Remote Manager.
7. The Web UI has been updated to no longer display deprecated cellular modem firmware images on the Modem status page.
8. The NTP server time.accns.com has been removed from the list of default NTP servers unless the aView management system is being used.
9. A new **system.log.persistent_path** configuration option has been added to allow the logs to be stored to a specific location including an external device like a USB flash drive.
10. The Web UI **System > Configuration Maintenance** page has been updated to improve the message displayed when an error is encountered when restoring a back configuration file.
11. The hostname of the device is now included in the OpenVPN client *.ovpn configuration file on the WebUI **Status > OpenVPN > Servers** page.
12. Support for connecting to the Cisco USB Console ports has been added.
13. The APN fallback list has been updated to remove the non-Internet type APNs.

SECURITY FIXES

1. The OpenSSL package on the TX64 has been updated to 3.0.2.
2. The OpenSSL package on the TX54 and LR54 platforms has been updated to 1.1.1o. [DAL-6303]
3. The Linux kernel has been updated to 5.17 [DAL-6081]
4. A Linux kernel patch for the “dirty pipe” vulnerability has been added. [DAL-5981]

   CVE-2002-0847 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P
5. The OpenVPN package has been updated to 2.5.6. [DAL-6229]

   CVE 2022-0547 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
6. The gcc tools have been updated to 11.2 and the binutils tools has been updated to 2.37. [DAL-5444]

   CVE-2019-15847 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N, CWE-331

   CVE-2018-12886 CVSS Score: 8.1 High CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-209

   CVE-2002-2439 CVSS Score 7/8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-190

BUG FIXES

1. An issue with the location support for devices configured with a non-UTC timezone which would report an incorrect UTC time when receiving TAIP messages. [DAL-6267. DAL-6335]
2. An issue with missing RSSI values for SSIDs for SSIDs found by the Wi-Fi Scanner when used on a Wi-Fi 6 module has been resolved. [DAL-6030]
3. An issue where an IPsec tunnel failing to reestablish the tunnel if the SAs are deleted after phase 1 re-authentication has been resolved. [DAL-4959]
4. An issue where the connection to Digi Remote Manager could be delayed up to 15 minutes before refreshing to use the active main WAN connection in the event of a network failover or failback has been resolved. [DAL-6164]
5. An issue with the default Wi-Fi AP SSIDs being too long on the TX64 Rail platform has been resolved. [DAL-6329]
6. An issue where OpenVPN > Advanced options > OpenVPN parameters text box was limited to 64 characters when synced with Digi Remote Manager has been resolved. The limited is now 64,000 characters. [DAL-6002]
7. An issue resulting from a race condition when disconnecting from Digi Remote Manager which could cause the Cloud Connector firmware to crash has been resolved. [DAL-5971]
8. An issue that could prevent Wi-Fi Hotspots from initializing correctly has been resolved. [DAL-6306, DAL-6313]
9. An issue that prevented an OpenVPN server from authenticating clients with an external LDAP, TACACS+ or RADIUS server has been resolved. [DAL-6159]
10. An issue that prevented LDAP external authentication for SSH and Telnet sessions has been resolved. [DAP-6098]
11. The **show containers** CLI command has updated to list all containers on the file system and not just those link to configuration settings.
12. Broken links on the Web UI for Digi Remote Manager on the Dashboard and **System > Digi Remote Manager** have been resolved. [DAL-6088]

13. An issue preventing an interface's MAC address **allowlist** from implicitly denying access to devices not in the allowlist has been resolved. [DAL-6001]
14. An issue with Python digidevice.config module which could result in a segmentation fault has been resolved. [DAL-6005]

VERSION 22.2.9.85 (March 2022)

This is a **mandatory** release.

NEW FEATURES

15. The internal GNSS module on the TX54 and TX64 platforms can now be used as a time source for the NTP server support.

ENHANCEMENTS

1. Added a SureLink option to switch SIMs if the SureLink tests fail for a configured number of times.
2. A set of new container CLI commands have been added to create, delete and interact with containers.
3. The default URL for Digi Remote Manager has changed to edp12.devicecloud.com.
4. The SCEP client support has been updated with two new settings to allow the user to configure a CA identity and the HTTP URL path for the CA.
5. A debug configuration option has been added to the IPsec support to allow the user to debug an IPsec tunnel.
6. A new serial port option has been added to send a configured string to a remote server when a TCP socket connection is opened on the serial port.
7. The location support has been enhanced with the following new settings
    - UDR support enable/disable (default: disabled)
    - Automatic attenuation enable/disable (default: enabled)
    - Minimum satellite signal level required for navigation (default: 6 dBHz)
    - Minimum number of satellites required for navigation (default: 3)
    - Maximum number of satellites required for navigation (default: 18)
8. The ability for policy-based routes to override the routing of packets through VPN tunnels has been added. This is useful in the case where you only want packets from a certain source network to go through the VPN tunnel.
9. A new TX54 and TX64 **system power ignition off_delay** CLI command has been added to allow the devices power off delay to updated without the configuration being updated. This means the next device reboot it will revert to its configured power off delay.
10. A new configuration setting has been added to allow the user to specify the minimum TLS version that can be used with the Web UI. By default, the minimum is TLS 1.2.
11. If a Sprint Curiosity SIM is being used, T-Mobile carrier firmware will now be used if available.
12. A new **cat** CLI command has been added for displaying the contents of a file.

SECURITY FIXES

1. The DNSMasq package has been updated to version 2.86 [DAL-5331]

CVE-2021-3448 CVSS Score: 4.0 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N

2. The OpenSSH package has been updated to version 8.8p1 [DAL-5451]
   CVE-2021-28041 CVSS Score: 7.1 High CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
   CVE-2020-14145 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3. The Linux kernel has been updated to 5.15 [DAL-5546]
4. The Busybox package has been updated to version 1.34.0 [DAL-5631]
   CVE-2021-42373 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42374 CVSS Score: 5.3 Medium CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H
   CVE-2021-42375 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42376 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42377 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42378 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42379 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42380 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42381 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42382 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42383 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42384 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42385 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42386 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
5. The dbus package has been updated to version 1.13.20 [DAL-5459]
   CVE-2020-12049 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-12749 CVSS Score: 7.1 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
6. The GRUB package has been updated to version 2.06 [DAL-5456]
   CVE-2021-3418 CVSS Score: 6.4 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
7. The bzip2 package has been updated to version 1.08 [DAL-5446]
   CVE-2019-12900 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2011-4089 CVSS Score: 4.6 Medium CVSS:2.0/AV:L/AC:L/Au:N/C:P/I:P/A:P
   CVE-2010-0405 CVSS Score: 5.1 Medium CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:P/A:P
8. The procps package has been updated to version 3.3.15 [DAL-5433]
   CVE-2018-1123 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-1124 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
   CVE-2018-1125 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-1126 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
9. The OpenSSL build has been updated to include secure compilation flags. [DAL-5472]

BUG FIXES

1. An issue where the TCP socket to location servers were not being properly closed between location messages has been resolved. [DAL-5716]
2. An issue that prevented the device from updating the maintenance window status with Digi Remote Manager if the maintenance window start time was between 00:00-00:59 has been

resolved. [DAL-5765]

3. An issue with IPsec where only the first policy would be setup on tunnels using IKEv2 has been resolved. [DAL-5347]
4. An issue preventing IPsec transport mode tunnels from initializing properly has been resolved. [DAL-5718]
5. An issue with SureLink DNS tests that could prevent an interface from coming up has been resolved. [DAL-5934]
6. An issue with QoS HFSC setup to limit bandwidth user for shared links has been resolved. [DAL-5814]
7. An issue preventing port forwarding firewall setups if the destination port(s) setting was left blank has been resolved. [DAL-5680]
8. An issue that where the TX54 and LR54 platforms failing to negotiate with some 10Mbps Ethernet switches has been resolved. [DAL-5506]
9. An issue with the Web UI allowing invalid Modbus client filter values to be configured has been resolved. [DAL-5905]
10. An issue with the Python digidevice SMS module where the callback stops working after a number of SMS messages have sent or received has been resolved. [DAL-5883]
11. An intermittent issue with the **show dhcp-leases** command where not all of the leases were being displayed has been resolved. [DAL-5688]
12. An issue preventing persistent containers from initializing has been resolved. [DAL-5847]
13. An issue with **sh: out of range** was being outputted when starting the test_lxc container has been resolved. [DAL-5845]
14. An issue with the CLI when a TACACS+ server is not configured correctly has been resolved. [DAL-5512]
15. An issue with interruptions of active serial port connections when changes are made to the serial port mode has been resolved. [DAL-5698]
16. An issue preventing MMS SMS message from being received and parsed properly, preventing large out-of-band configuration changes from being from aView/ARMT has been resolved. [DAL-5538]

VERSION 21.11.60.63 (December 2021)

This is a **mandatory** release.

NEW FEATURES

1. A new firmware update option has been added to allow the device to be automatically updated when a new firmware version is available has been added.
2. Support for **TACACS+ authorization and accounting** for Admin CLI commands had been added.
3. Support for **certificated based WPA2/WPA3 authentication for Wi-Fi client connections** has been added.

ENHANCEMENTS

1. The SureLink support has been enhanced as follows:

- A new **Cellular SureLink** configuration option to allow the Cellular module to be reset after a specified number of SureLink test failures.
- A new **show surelink** CLI command has been added to display the status of the SureLink tests for an interface or VPN tunnel.

2. A new **NMEA Talker ID** configuration option has been added to the **Location > Destinations** configuration. The default is "GN".
3. The default value for the **IPsec IKE Diffie Hellman group** has been changed to **group 14** for enhanced compatibility for industry standard settings.
4. The default value for the **serial port history** has been changed to **disabled** when in remote access mode.
5. The "-" and "." characters can now be used in authentication username configuration.
6. A **show containers** CLI command for listing details of configured containers has been added.
7. The Wi-Fi Scanner configuration has been updated to automatically configure the underlying client mode settings.
8. The Airmob **datapro** APN has been added to the APN fallback list.
9. The SIM ICCID and phone number are now included in a Digi RM query_state response.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **9.8 Critical**.

1. The Python version has been updated to 3.6.15. [DAL-3190]
   CVE-2021-3177 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2. The Linux kernel has been updated to 5.14. [DAL-5360]
3. The OpenSSL package has been updated to 1.1.1l. [DAL-5242]
   CVE-2021-3711 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-3712 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H
4. The OpenVPN package has been updated to 2.5.4. [DAL-5435]
   CVE-2021-3824 CVSS Score: 6.1 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
   CVE-2020-15078 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
5. The busybox package has been updated to 1.33.1. [DAL-5290]
   CVE-2021-28831 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
6. The stunnel package has been updated to 5.60. [DAL-5291]
   CVE-2021-20230 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
7. The libunbound library has been updated to 1.13.2. [DAL-5420]
   CVE-2020-12663 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2020-12662 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-25042 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2019-25041 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-25040 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-25039 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2019-25038 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2019-25037 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-25036 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2019-25035 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2019-25034 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2019-25033 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2019-25032 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2019-16866 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

8. The libidn2 library has been updated to 2.3.2. [DAL-5439]

   CVE-2019-18224 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-12290 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

   CVE-2017-14062 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2017-14061 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2016-6263 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2016-6262 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

   CVE-2016-6261 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2015-8948 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

   CVE-2015-2059 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P

9. The muslv package has been updated to 1.2.2. [DAL-5452]

   CVE-2020-28928 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

10. The rsync package has been updated to 3.2.3. [DAL-5431]

    CVE-2018-5764 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

    CVE-2017-17434 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

    CVE-2017-15994 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

    CVE-2014-2855 CVSS Score: 7.8 High CVSS:2.0/AV:N/AC:L/Au:N/C:N/I:N/A:C

    CVE-2006-2083 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P

BUG FIXES

1. An issue that prevented IPsec tunnels from being setup properly if the tunnel name was longer than 9 characters has been resolved. [DAL-5139]
2. An issue where the firewall from working correctly when a port forwarding rule was configured with the protocol type **other** has been resolved. [DAL-5501]
3. An issue where the mode indicator field in forwarded NMEA messages was missing when there was no GNSS fix has been resolved. [DAL-5464]
4. An issue with the formatting of the **Cellular health metrics** has been resolved. [DAL-3994]
5. An issue with the **show modem name <name>** command that could cause a multi-minute delay has been resolved. [DAL-5297]
6. An issue with **SureLink ping tests** using the same source IP address on different network interfaces using the same physical port. [DAL-5478]
7. An issue with **SureLink reboot action** not taking working if the SureLink restart interface action was also enabled has been resolved. [DAL-5485]
8. An issue with the Web UI not being able to create new configuration elements with dynamic name arrays has been resolved. [DAL-5481]
9. The cellular module manufacturer has been removed the Web UI and CLI modem status. [DAL-5171]

10. An issue with the Python **digidevice.maintenance** module were the service state was not correctly initialized has been resolved. [DAL-5462]
11. An issue with the Python **digidevice.config** module that prevented multiple configuration changes from being applied has been resolved. [DAL-5192]
12. An issue with the Python **digidevice.runt** module that could cause a segmentation fault when getting a runt value after previously setting it has been resolved. [DAL-5468]
13. An issue that prevented IPsec tunnels from being setup in Transport mode has been resolved. [DAL-5490]
14. An issue that prevent the **on boot** SIM preference schedule from taking effect has been resolved. [DAL-5547]

VERSION 21.8.24.139 (October 2021)

This is a **mandatory** release.

ENHANCEMENTS

1. The location forwarding support has been updated as follows
    - NMEA sentences now use the GP prefix instead of the GN prefix. This will be configurable in the 21.11 release.
    - When using TCP connections to forward the location data, the TCP connections will remained connected in between updates rather than being closed and reopened. If the connection is closed by the remote TCP server, the connection will be automatically re-established by the device.

BUG FIXES

1. The following issues in the 21.8.24.129 release have been resolved:
    - Cellular connections not being established on the LR54/LR54W platforms. [DAL-5346]
    - LR54 SIM1 and SIM2 LEDs not correctly being lit. [DAL-5367]
    - The WWAN Signal and Service flashing every 30 seconds. [DAL-5269]
4. An issue where “out of range” messages that were being displayed out in the shell console when uploading device health metrics on the TX64 has been resolved. [DAL-5324]

VERSION 21.8.24.129 (September 2021)

This is a **mandatory** release.

NEW FEATURES

5. **LXC container** support for running localized containers on the router has been added.
6. **5G Standalone (SA)** support has been added to the TX64 5G and TX64 Rail platforms.
7. Support for **802.1x port based network access control** has been added.
8. Support for **L2TPv3 VPN tunneling** (client and server) has been added.
9. A new **monitoring metrics upload** CLI command has been added to upload the health metrics to Digi RM on demand.
10. A new **system script start** CLI command and Web UI **Status > Scripts** page has been added to

allow the user to manually start scripts that are configured under **System > Scheduled tasks > Custom scripts** with a run mode of manual

11. A new **speedtest** CLI command has been added to run either an Iperf or Nuttcp performance test with a remote server.
12. A new **system time** CLI command has been added to allow the device's time to be manually set.
13. A new **system find-me** CLI command and Web UI **Status > Find Me** button that will flash the device's LEDs to allow the device to be located has been added.

ENHANCEMENTS

1. The maintenance window support has been updated to allow multiple triggers to be configured. Each trigger can be based on a time window, an interface status or a Python API. When the device enters or leaves its maintenance window, it will notify Digi RM, which will allow or prevent scheduled tasks to run based on the status.
2. Support for IPsec IKE fragmentation has been added.
3. The network bridging support has been enhanced to support VLAN networking where a bridge becomes a virtual switch. The switch can route packets across VLAN trunks to get true layer 2 networking on VLANs.
4. The firewall support has been updated to allow or deny Ethernet packets based on source and destination MAC addresses.
5. The **Digi RM Files > Persistent files** folder, the **system backup** CLI command, and Web UI **System > File System** page have been updated to allow for the setting of custom default configuration via a /opt/custom-default-config.bin file.
6. The ability to delete a custom default configuration by performing a double erase sequence has been added.
7. The Wi-Fi scanner support has been updated to include additional filtering capabilities including Client or Access Point only, MAC address and partial MAC address filtering, RSSI thresholds and static device detection.
8. The Wi-Fi support has been updated to so that the default SSID and passphrase does not need to be changed when saving configuration changes.
9. The option for uploading device event logs to Digi RM has been added.
10. The Python **digidevice datapoint** module has been updated with the **upload_multiple** function to allow multiple datapoints to be uploaded to Digi RM.
11. The **system support-report** CLI command has been updated to store the support report file to /var/log unless an alternate path is given. It will also provide help text in how to upload the support report file to a remote server using SCP.
12. A new **Network > Advanced > Sequential DHCP address allocation** configuration setting has been added to allow DHCP addresses to be assigned sequentially or randomly. The default is randomly.
13. A new **clear dhcp-lease** CLI command has been added to allow all or specific DHCP leases to be cleared based on IP address or MAC address.
14. The Wi-Fi auto-channel selection on the 5GHz band has been updated to help avoid channel congestion.
15. The CLI login help text has been updated to include common tool tips.

16. The user configuration had been updated to require the user to be assigned to at least one group to help prevent a misconfiguration where a user is configured but does not have any permissions.
17. Support for configuring multiple destination networks and interfaces for multicast routes has been added.
18. New SSH custom configuration has been added to override or edit the SSH server options.
19. The ability to upload files to the /opt and /etc/config/analyzer directories via Digi RM and the Web UI has been added.
20. The Digi RM keepalive messages have been updated to prevent delays in keepalive responses.
21. The cellular modem manufacturer name has been removed from the UI and health metrics.
22. The cellular TAC location has been added to the metrics reported to Digi RM.
23. The list of pre-defined cellular APNs that the device will attempt to use if no APNs are configured has been shortened by removing wildcard entries.
24. The local date and time is now persistent across reboots once a successful NTP sync has occurred.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **8.1 High**.

1. An STS header has been added to the HTTPS Web UI. [DAL-4991]
2. The libcurl package has been updated to 7.76.0 [DAL-4774]

   CVE-2021-22897 CVSS Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

   CVE-2021-22898 CVSS Score: 3.1 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

   CVE-2021-22901 CVSS Score: 8.1 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

BUG FIXES

1. An issue with the **modem pin status** CLI command has been resolved. [DAL-5056]
2. An issue where Digi RM would remediate a device every time it is scanned due to the local user passwords being hashed has been resolved. [DAL-4974]
3. An issue where the **system restore** CLI command could default the device if the configuration backup file was stored in the /etc/config directory has been resolved.
4. Python PIP has been updated to 21.2.4 to resolve an issue when installing python modules needing PEP517 hooks. The default user-base directory has been set to /etc/config/scripts so that python pip can install module dependencies to a writeable location when **pip install --user <module_name>** is used. [DAL-5068]
5. An issue where the mDNS service would occasionally crash has been resolved. [DAL-4663]
6. An issue with the Web API where configuration with spaces or array configuration not being allowed has been resolved. [DAL-5039, DAL-4895]

VERSION 21.5.56.106 (June 2021)

This is a **mandatory** release.

NEW FEATURES

1. Support for **Wi-Fi WPA3** security has been added. The following new modes are supported:
   - WPA2/WPA3 Personal

- WPA3 Enhanced Open
- WPA3 Personal
- WPA3 Enterprise (only on TX64 radio 2)

14. Support for **Wi-Fi WPA** and **WPA/WPA2** mixed modes with **TKIP** has been added. This is not available on PR platforms.
15. Support for multiple IPsec peers have been added. The peers can be tried either in a round-robin or random sequence in order to establish an IPsec tunnel.
16. Options to control the IPsec IKE negotiations with respect to retransmits and timeouts have been added to better handle IPsec connection failures.
17. The **SureLink** support has the following new features
    - Support for separate configurable number of SureLink test failures to occur before the Restart or Reboot actions are taken.
    - Support for a configurable number of SureLink test passes to occur before a network interface is marked as working.
    - The ability for a network interface to test whether another network interface is either up or down and has IP connectivity.
18. Support for **SNMPv2c** has been added.
19. A new **UDP serial mode** has been added to the Serial port configuration which allows serial-over-UDP connections.
20. A new Autoconnect feature for Serial ports in Remote Access mode that support raw TCP connections, SSH, Telnet, and encrypted connections with and without authentication has been added.
21. A default **digi.device** local domain name has been added for the default 192.168.210.1 interface to allow for easier SSH and Web UI access.

ENHANCEMENTS

1. Support for doing a **cellular modem firmware update** via Digi Remote Manager has been added.
2. Support for doing a **speed test** via Digi Remote Manager has been added.
3. A new **modem scan** Web UI page has been added that allows users to scan for available carriers and then lock the device to a particular carrier.
4. An option to add a random delay to a scheduled reboot time has been added.
5. Support for Read-Only CLI access via Digi Remote Manager has been added.
6. The requirement to change the device's default password for the admin user when the device is first configured has been removed.
7. The **Firewall > Port Forwarding** support has been updated to support a range of ports including 1:1 and many-to-one port mappings.
8. The **network analyzer filtering** support has been updated to allow for easier configuration for filtering on IP addresses and networks, TCP/UDP ports, IP protocols, MAC addresses and VLANs.
9. A **LDAP login attribute** option has been added to control the attribute ID used so it can match with the attribute set in an Active Directory server.
10. The Auto-APN detection is now skipped for **Deutche-Telekcom** SIMs and the **internet.telekon**

APN is used by default.

11. The T-Mobile **internet.gma.iot** APN has been added to the APN fallback list.
12. The network interface MAC address filtering options have been renamed to **AllowList** and **DenyList**.
13. A **system firmware ota** CLI commands have been updated to check, list and update the devices firmware from the Digi firmware server.
14. The **show dhcp-lease** CLI command has been updated to be more descriptive.
15. A **show dns** CLI command has been added to display the active DNS server for each interface.
16. A **show ntp** CLI command has been added to display the NTP status.
17. The LWM2M parameters have been updated to include the AT&T Host IDs for the EM9191, LM940 and LM960 cellular modems.
18. A step has been added to the reboot process to correctly power off the EM9191 module.
19. The error messages that are displayed if an error occurs when downloading system or modem firmware have been updated to provide more detailed information.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **9.8 Critical**.

1. The Python version has been updated to 3.6.13. [DAL-3190]
2. The OpenSSL package has been updated to 1.1.1k [DAL-4755]
   CVE-2021-23840 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-23841 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-3449 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-3450 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
3. The libcurl package has been updated to 7.76.0 [DAL-4774]
   CVE-2021-22876 CVSS Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
   CVE-2021-22890 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
4. The netsnmp package has been updated to 5.9 [DAL-4669]
   CVE-2018-18066 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-18065 CVSS Score: 6.5 Medium CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2015-5621 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P
   CVE-2014-3565 CVSS Score: 5.0 Medium CVSS:2.0/AV:N/AC:L/Au:N/C:N/I:N/A:P
   CVE-2014-2284 CVSS Score: 5.0 Medium CVSS:2.0/AV:N/AC:L/Au:N/C:N/I:N/A:P
   CVE-2014-2285 CVSS Score: 4.3 Medium CVSS:2.0/AV:N/AC:M/Au:N/C:N/I:N/A:P
   CVE-2012-6151 CVSS Score: 4.3 Medium CVSS:2.0/AV:N/AC:M/Au:N/C:N/I:N/A:P
5. The tcpdump package has been updated to 4.99.0 [DAL-4587]
   CVE-2018-10103 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2018-10105 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2018-14461 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14462 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14463 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14464 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14465 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14466 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14467 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-14468 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2018-14469 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-14470 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-14879 CVSS Score: 7.0 High CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
CVE-2018-14880 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-14881 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-14882 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16227 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16228 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16229 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16230 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16300 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16451 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2018-16452 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2019-15166 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

6. The libpcap package has been updated to 1.10.0 [DAL-4587]
   CVE-2019-15163 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-15161 CVSS Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
   CVE-2019-15164 CVSS Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
   CVE-2019-15165 CVSS Score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
7. The minimum length requirement for user passwords has been reduced to 8 characters, except for PR platforms that have a minimum length requirements of 10 characters
8. The listening services such as SSH, Web UI, DNS have been reduced to the lowest privilege level. [DAL-4703]
9. Support for the following SSH algorithms have been removed
   - MAC algorithms
     - umac-64-etm@openssh.com
     - hmac-sha1-etm@openssh.com
     - umac-64@openssh.com
     - hmac-sha1
   - Key Exchange algorithms
     - diffie-hellman-group14-sha256
     - diffie-hellman-group16-sha512
     - diffie-hellman-group18-sha512

BUG FIXES

1. An issue that was preventing some **TX54-A112** devices (with serial numbers TX54-XXXXXX) from saving configuration settings due to incorrect file system partition has been corrected. [DAL-4866]
2. An issue with overlapping 5GHz Wi-Fi ranges that caused Access Point and Client conflicts when connecting has been resolved. [DAL-4733]
3. An issue when authenticating users if multiple TACACS+ servers are configured and the first server is unresponsive has been resolved. [DAL-4748]
4. An issue that prevented the TX54 and TX64 from automatically connected to T-Mobile in Hungary has been resolved. [DAL-4679]

5. An issue where multiple VRRP instances are configured with VRRP+ that did not become VRRP master has been resolved. [DAL-4824]
6. An issue where outbound SMS messages could not be sent using various carrier SIM cards has been resolved. [DAL-4794]
7. An issue where a device could stop participating in RIP routing if the network interfaces are reset has been resolved. [DAL-4704]
8. An issue where RIP, BGP and other routing protocols would not start properly if the configuration is updated has been resolved. [DAL-4704]
9. An issue that prevented default routes being advertised via RIP has been resolved. [DAL-4799]
10. An issue that prevented GRE interfaces from being specified with BGP and other routing protocols has been resolved. [DAL-4695]
11. An issue that prevented VPN tunnels from being specified within port forwarding rules has been resolved. [DAL-4524]
12. An issue the prevented access to multiple remote networks through an IPsec tunnel with the same policy has been resolved. [DAL-4816]
13. An issue where the network analyzer could be stopped in the CLI when a Ctrl-C was issued for a different command has been resolved. [DAL-4652]
14. An issue with the OpenVPN client Web UI page incorrectly displaying the tunnel status has been resolved. [DAL-4357]
15. An issue where location based health metrics not being uploaded to Digi Remote Manager has been resolved. [DAL-4310]
16. An issue that prevented configuration when being “pasted” into the CLI when using the output of the **show config cli-format** command has been resolved.
17. An issue that prevented the **signal** aView/ARMT command from triggering the device to send signal strength logs has been resolved. [DAL-4915]
18. The proper return status code for custom scripts configured on the device is now returned. Previously the exit code was always 0. [DAL4670]

DEPRECATION

1. The Babel routing service is no longer supported.

VERSION 21.2.39.67 (March 2021)

This is a **mandatory** release.

NEW FEATURES

1. Geofence support has been added. The user can configure multiple different circular or polygonal geofences and have the device take a configurable action when it leaves or enters a geofence.
22. A new **modem scan** CLI command has been added to allow the user to scan for available carriers. Configuration has also been added to lock the device to a particular carrier.
23. A REST API has been added that allows the user to get and set configuration.

ENHANCEMENTS

1. The Wi-Fi support has been updated to support DFS channels in client mode. A DFS-Client

mode must be set on the Wi-Fi module in order to access DFS channels 149, 153, 157, 161 and 165.

When in the DFS-Client mode, any Access Points configured on the Wi-Fi module will be disabled.

24. The Wi-Fi 5GHz channels 36, 40, 44 and 48 have been added to the Wi-Fi background scanning support. Also the default settings for the Wi-Fi background settings to be update to be
    - Scan Threshold : -75
    - Short Interval : 5
    - Long Interval : 300
25. The default bandwidth for Wi-Fi 2.4GHz channels has been set to 20MHz.
26. The SureLink recovery of Wi-Fi connections was updated to restart the Wi-Fi module if restarting the network connections fails to recover the connection.
27. The IPsec support has been updated to support asymmetric pre-shared keys with IKEv2.
28. The location support has been updated to allow a user-defined latitude, longitude and altitude to be configured for the device's location.
29. The location forwarding support has been updated to support sending data over a TCP connection and to have a separate interval configuration.
30. The location support has been updated to send the device's location to Digi Remote Manager as soon as it gets a valid GNSS fix.
31. The IPsec connection uptimes are now being uploaded to Digi Remote Manager as part of the metrics.
32. The IPsec support has been updated so that Aggressive/Main mode or Xauth configuration is not displayed if IKEv2 is selected.The iptables TRACE command has been added to for enhanced firewall debugging.
33. Support for running remote CLI commands from Digi Remote Manager have been added.
34. The TX54 reboot functionality has been enhanced to power cycle the USB peripherals.
35. The OpenVPN client and server public key and private key configuration have been changed to Client_certificate, Server_certificate and Server_key to make clearer of their use.
36. The accuracy of the modem status has been improved during a firmware update.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **8.1 High**.

1. The Python version has been updated to 3.6.12. [DAL-4364]

   CVE-2020-14422 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
2. The OpenSSL package has been updated to version 1.1.1i. [DAL-4326]

   CVE-2020-1971 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3. The DNSMasq package has been updated to version 2.83. [DAL-3950]

   CVE-2019-14834 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
   CVE-2020-25681 CVSS Score: 8.1 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2020-25682 CVSS Score: 8.1 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2020-25683 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2020-25684 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
   CVE-2020-25685 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

CVE-2020-25686 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
CVE-2020-25687 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

4. The hostapd package has been updated to resolve critical issues. [DAL-4232]
   CVE-2019-16275 CVSS Score: 6.5 Medium CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-13377 CVSS Score: 5.9 Medium CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
37. The WPA supplicant package has been updated to resolve critical issues. [DAL-4233]
   CVE-2019-16275 CVSS Score: 6.5 Medium CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
38. The libcurl package has been updated to version 7.74.0. [DAL-4234, DAL-4366]
   CVE-2020-8169 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
   CVE-2020-8177 CVSS Score: 7.1 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
39. The Web server security has been updated with the following headers:
    - Pragma: no-cache
    - Content-Security-Policy
    - X-Content-Type-Options: nosniff
    - X-XSS-Protection: 1; mode=block
    - X-Frame-Options: SAMEORIGIN set to uppercase

   [DAL-4192]
40. Automatically deactivate active user logins/sessions if the password for that user changes. [DAL-4362]
41. Removed support for HTTPS CBC ciphers. [DAL-4408]
42. Removed debug configuration options for PR firmware for changing HTTPS ciphers. [DAL-4417]
43. An XSS vulnerability on the serial page in the Web UI has been resolved. [DAL-4646]

BUG FIXES

1. An issue has been resolved where the non-primary DNS servers were queried through the wrong interface when the **use_dns** configuration option was set to **primary**. [DAL-3156]
2. An issue where a Wi-Fi Access Point would not make a client connection on 2.4GHz has been resolved. [DAL-3943]
3. An issue on the TX54 where the cellular module disconnects with a “modem not available” error has been resolved. [DAL-4423]
4. An issue that prevented Web UI access when two-factor authentication was enabled has been resolved. [DAL-4509]
5. An issue where an incorrect format of ICCID and IMEI metrics were being sent to Digi Remote Manager has been resolved. Also the phone number of the SIM is now included in the metrics. [DAL-4440]
6. An issue with an aView initiated speed test reporting the same upstream/downstream values has been resolved. [DAL-4420]
7. An issue that prevented the LM940 cellular module from reconnecting after a module firmware update has been resolved. [DAL-2933]
8. An issue when using IPsec configured to use the default route for the local endpoint has been resolved. [DAL-4433]
9. An issue where a cellular module firmware update on dual cellular platforms which could

result in the wrong module being updated has been resolved. [DAL-4189]

10. An issue with Wi-Fi LEDs on the TX54 Dual Wi-Fi variants has been resolved. [DAL-4185]
11. An issue where a hotspot would stop responding to DHCP requests if the hotspot was started many times has been resolved. [DAL-4298]
12. An issue with the syslog configuration when updating from the DAL 20.5 release to DAL 20.8 or DAL 20.11 release has been resolved. [DAL-4426]
13. An issue preventing configuration updates via Digi Remote Manager if SCEP settings were enabled on the device have been resolved. [DAL-4445]
14. An issue with the **show wifi ap name <name>** and **show wifi client name <name>** CLI commands has been resolved. [DAL-1615, DAL-1616]
15. An issue where an incorrect system uptime is displayed in the Web UI and **show system** CLI command has been resolved. [DAL-4350]
16. An issue where CLI sessions showing stale configuration settings if the device was updated in a different session has been resolved. [DAL-2284, DAL-2671, DAL-4446, DAL-4530]
17. The message displayed in the Web UI after factory defaulting a device has been updated to direct the user to refresh the page. [DAL-2326]
18. An issue where dynamic DHCP leases were not been displayed in the Web UI or CLI has been resolved. [DAL-4557]
19. An incorrect Ethernet interface status when the device is in passthrough mode has been fixed. [DAL-4543]
20. An issue that prevented use of the Python digidevice.config module in PR firmware images has been resolved. [DAL-4378]
21. An issue with software flow control on serial ports configured in remote access mode has been resolved. [DAL-3630]
22. A timing issue with the LM940 modem that prevented the modem from reconnecting after a firmware update has been resolved. [DAL-4614]
23. A SureLink issue that could prevent a second APN connection if the interface was configured with just an **Interface Up** test has been resolved. [DAL-4629]
24. A rare issue where the Digi RM client could crash when making a configuration change has been resolved. [DAL-4593]

VERSION 20.11.32.138 (December 2020)

This is a **mandatory** release.

NEW FEATURES

1. Support for the following Primary Responder (PR) platforms has been added
    - TX54-Single-Cellular-PR (TX54-A146)
    - TX54-Dual-Cellular-PR (TX54-A246)
    - TX64-PR (TX64-A141)

44. The IPsec support has been updated to use XFRM interfaces which allows IPsec tunnels to be treated like network interfaces which allows them to be used for static routes, policy-based routes, access control lists, routing based on metrics, etc.
45. Support for IPv6 IPsec tunnels, IPv6-over-IPv4 and IPv4-over-IPv6 tunneling has been added.

46. Support for Python PIP module for installing external libraries and modules has been added.
47. A new **modem firmware** CLI command for performing local and over-the-air remote firmware updates on the cellular modem(s) on the device.
48. Ethernet configuration for duplex and speed has been added.
49. An option to starting, stopping and viewing serial port activity logs via the CLI, Web UI and Digi RM has been added.

ENHANCEMENTS

1. The **m2m.telus.iot** Telus APN has been added to the APN fallback list.
2. The **890103** and **890141** ICCID prefixes and **31030** PMND ID matchers to the AT&T APN fallback list.
3. The **psmtneorm** and **edneopate010.dpa** APNs have been added to the AT&T APN fallback list.
4. The **reseller** and **tracfone.vzwentp** APNs have been added to the Verizon APN fallback list.
5. The IPsec support has been updated so that the device will wait for Surelink tests (if configured) to pass before initiating outbound IPsec tunnels.
6. The QXDM support has been updated to support encrypted QXDM access to the cellular modem on the device. Note that this is always enabled on the PR platforms.
7. **SSH** and **telnet** CLI commands have been added. Note that the telnet command is not available on the PR platforms.
8. The VRRP support has been updated to use virtual MAC addresses on the LAN interface.
9. A **defaultroute** option has been added for matching policy based router to the device's active default route.
10. A **DSCP** option has been added to policy based routes to allow users to match the routing rule to the type of DSCP field in the packet.
11. A **Services > Ping Responder** configuration has been added for controlling what interfaces and firewall zones the device will respond to ICMP requests on.
12. A **Modbus Gateway** status CLI command and Web UI page have been added,
13. The IPsec support has been updated to hide to the Main / Aggressive Mode configuration if IKEv2 has been selected. [DAL-4142]
14. A **scripts** status CLI command and Web UI page have been added that allow the user to manage scripts that running on the device.
15. The **show modem** CLI command has been updated to display if the modem is switching firmware.
16. The **Monitoring > Device Health** configuration will now be hidden if the Digi RM management has been disabled.
17. The network bridge support has been updated to use the MAC address of the first configured device in the bridge for the bridge interface.
18. The following modem firmware and SIM details are uploaded to Digi RM as part of the health metrics:
    - SIM PLMN
    - SIM IMSI
    - SIM Provider
    - Modem IMEI

- Modem Manufacturer
- Modem Model
- Modem Revision
- Modem CNTI
- Modem Connection Status

19. A system log entry is added if the Surelink DNS tests are skipped if the interface does not have any DNS servers.
20. The Web UI has been updated with several enhancements:
    - The Ethernet interface speed configuration has been updated with correct notation.
    - The dashboard will now display the cellular technology icon for the service being used.
    - The dashboard will now display the Digi RM connection time in a finer granularity.
    - The dashboard has been updated with some formatting changes.
    - Help button added to File System page which links to the relevant User Guide section.
    - The Modem Firmware Update page now has a link to the scheduled maintenance page.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **9.1 Critical**.

1. A tcpdump memory allocation issue have been resolved. [DAL-4226]
   CVE-2020-8037 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2. The jQuery package has been updated to 3.5.0.
   CVE-2020-11022 CVSS Score: 6.1 Medium 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
   CVE-2020-11023 CVSS Score: 6.1 Medium 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3. The OpenVPN package has been updated to 2.4.9
   CVE-2018-7544 CVSS Score: 9.1 Critical 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
4. The Bash package has been updated to 5.0
5. The OpenSSH package has been updated to 8.3p1
6. The OpenSSL package had been updated to 1.1.1h
7. Updates have been made to prevent command injection through modem firmware update web pages. [DAL-4046, DAL-4093, DAL-4104]
8. An issue where some file could be downloaded from the device without authentication has been fixed. [DAL-3835]
9. An issue where it was possible to add files to the encrypted file system on the TX64 if you had physical access has been fixed. [DAL-4149]
10. The Web UI has been updated to prevent authentication in HTTP GET requests. [DAL-3834]
11. The Web UI has been updated to set the Content-Security-Policy header. [DAL-3629]
12. The firmware update process has been updated to further firmware validation. [DAL-3511]
13. TCP forwarding from incoming SSH connections have been disabled. [DAL-3938]

BUG FIXES

1. An issue that resulted in the delayed sending of health metrics to Digi RM has been resolved. [DAL-3908]

2. An issue with IPsec and OpenVPN Surelink recovery actions failing if the tunnel name is longer than 7 characters have been resolved.
3. An issue with policy based routing not working in conjunction with multiple IPsec tunnels has been fixed. [DAL-3515]
4. The format of user passwords when displayed in Digi RM has been fixed. [DAL-3889]
5. An issue that prevented firewall rules from being setup for OSFPv2 entries has been fixed. [DAL-3869]
6. An issue that prevented multicast traffic from being sent through a GRE tunnel has been fixed. [DAL-3879]
7. An issue that prevented OpenVPN clients using auto-generated configuration files from a TAP-bridge OpenVPN server has been fixed. [DAL-3881]
8. An issue that prevented OpenVPN server managed certificates from being re-generated if the process was interrupted has been fixed. [DAL-3803]
9. An issue with VRRP+, where the device could become the VRRP Master before any of the monitored interfaces come up has been resolved. [DAL-4274]
10. An issue with the Wi-Fi Scanner that prevented the scanner logs from being listed on the **System > Logs** page unless static filtering was enabled has been fixed. [DAL-3817]
11. An issue with Digi RM configuration profiles missing an option for setting the **SIM Slot Preference** has been fixed. [DAL-3912]
12. An issue where not all default configuration values where being uploaded to Digi RM which lead to problems with the Configuration Manager has been fixed. [DAL-3789]
13. The **system disable-cryptography** command has been fixed. [DAL-4169]
14. An issue where the /opt file system space being incorrectly displayed in the **show system verbose** command has been fixed. Other formatting change has also been made. [DAL-3702, DAL-3805]
15. An issue with the factory default second stage erase not working has been fixed. [DAL-3944]
16. Duplicate modem signal information on the Web UI **Modem > Status** page has been removed. [DAL-3680]

VERSION 20.08.22.32 (September 2020)

This is a **mandatory** release.

NEW FEATURES

1. Verizon DMNR support has been added.
50. Serial Modbus gateway support has been added.
51. VRRP+ support to allow a VRRP backup to monitor the VRRP master has been added.
52. Python support sending and receiving SMS messages has been added.
53. MQTT client support has been added via the Python Paho module.
54. Ethernet network bonding to allow the same MAC address and IP configuration to be shared for multiple physical Ethernet ports in either active/backup or round robin mode.
55. Support for custom factory configuration has been added.
56. Support for the Digi aView cloud service has been added.

ENHANCEMENTS

1. The device health metrics support has been updated as follows:
    - Only upload health metrics to DRM that have changed since it was last uploaded. Note that all health metrics are uploaded at least once an hour.
    - Allow the user to configure which health metrics are uploaded to DRM
    - The format of the health metrics have been updated to reduce the bandwidth used when being uploaded to DRM.
2. The cellular firmware update on the TX54 and TX64 platforms has been updated as follows:
    - Allow the cellular module not being updated to continue to operate as normal
    - Prevent both cellular modules being updated at the same time
3. The number of maximum Wi-Fi connections supported by the TX64 Wi-Fi 2 module has been increased to 128.
4. The Wi-Fi support has been updated to support multiple RADIUS servers for WPA2 Enterprise security.
5. The Wi-Fi support has been updated to allow the transmit power to be configured. By default, the Wi-Fi module transmit at 100%.
6. A new Authoritative option has been added under TACACS+, RADIUS and LDAP user authentication configuration to prevent other authentication methods from being used if the given user credentials are invalid.
7. The Syslog support has been updated to allow UDP/TCP and port to be configured.
8. The Serial TCP connection support has been updated to allow encrypted/non-encrypted connections to be configured.
9. The Serial TCP/Telnet/SSH connection support has been updated to allow TCP keepalive messages and nodelay to be configured.
10. The NTP support has been updated to use a random unprivileged port for NTP time syncs if standard port 123 fails.
11. The location support on been updated to favor an external GNSS device over the internal GNSS module if both have valid fixes.
12. The ability to copy the running firmware image into the secondary firmware partition has been added. This can be done via the Web UI **Firmware Update** page or and **system duplicate-firmware** CLI command.
13. A new Web UI **Status > VRRP** status page and **show vrrp** CLI command has been added.
14. A new Web UI **Status > Scripts** page and **show scripts** and **system script stop <script name>** CLI commands have been added to show and manually stop any custom scripts or applications.
15. The Web UI Hotspot status page and **show hotspot** CLI command have been updated to include the current hotspot status.
16. The Web UI support has been updated to fade out the **Configuration saved** message to fade out.
17. The **update firmware** CLI command has been moved to be under **system**.

SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of 6.7 Medium.

1. The Linux kernel has been updated to 5.7 [DAL-3322] CVE-2020-10732 CVSS Score: 4.4 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L
57. Admin user login rate limiting has been added to prevent additional login attempts for 15 minutes by default after 5 failed attempts. [DAL-3390] CVSS Score: 6.7 Medium CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
58. /etc/config/start has been prevented from running when the shell is disabled. [DAL-2846] CVSS Score: 5.2 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:L
59. The Web UI has been updated to prevent file path extension on the Firmware Update and File System pages. [DAL-3471, DAL-3513, DAL-3518] CVSS Score: 3.2 Low CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
60. The Web UI has been updated to prevent cross-site scripting on the Wi-Fi and Bluetooth scanning pages. [DAL-3628] CVSS Score: 3.8 Low CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
61. The boot process for the TX54 and LR54 has been updated to prevent it from being interrupted. [DAL-3590] CVSS Score: 4.2 Medium CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
62. The SIM PIN configuration has been updated so that it can no longer be displayed in cleartext. [DAL-3462] CVSS Score: 3.2 Low CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N
63. The Web UI HTTP authentication cookie has been set as secure. [DAL-3393] CVSS Score: 3.1 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
64. File descriptor leaks on Serial connections has been fixed. [DAL-3202]

BUG FIXES

1. An issue which prevented RADIUS or TACACS+ authentication from working if local authentication was not enabled has been resolved. [DAL-3701]
2. An issue where IPsec tunnels with multiple policies configured would only properly route traffic for the last policy has been resolved. [DAL-3448]
3. An issue preventing a network interface from initializing if the interface name was longer than 7 characters has been resolved. [DAL-2327]
4. An issue preventing WAN passthrough mode from working if the WAN interface is configured with a static IP address has been resolved. [DAL-3097]
5. An issue preventing VLANs from being assigned to Wi-Fi SSIDs has been resolved. [DAL-3113]
6. An issue causing errors to be displayed on the CLI when configuring a USB serial port in remote access mode has been resolved. [DAL-3207]
7. An issue preventing users from configuring an IP address as a remote syslog server has been resolved. [DAL-3433]
8. An issue preventing cellular connectivity if a custom gateway/subnet is configured and the device is not in passthrough mode has been resolved. [DAL-3585]
9. An issue where an incorrect **Age of Data Indicator** value was being reported in TAIP messages has been resolved. [DAL-3249]
10. The **show system** CLI command has been updated to correctly display the CPU usage statistics. [DAL-2540]
11. The **show manufacture** CLI command has been updated to correctly display the MCU version. [DAL-3655]

12. The **modem sim-slot show** CLI command has been updated to correctly display the active SIM slot when SIM slot is in use. [DAL-3569]
13. An issue where the **mmcli** shell command would report an invalid SIM slot has been resolved. [DAL-3481]

VERSION 20.5.38.58 (July 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. The minimum requirements for a local user password has been changed to require the following:
    a. A minimum of 10 characters.
    b. At least one uppercase letter.
    c. At least one lowercase letter.
    d. At least one number.
    e. At least one symbol.

SECURITY FIXES

1. Failed login attempts have been added to the event log and will sent to a remote syslog server if enabled. [DAL-3492]

BUG FIXES

65. An issue that caused a delay in connecting with FirstNet SIMs has been resolved. [DAL-3236]
66. An issue that prevented dual APN connectivity with AT&T when using Sierra Wireless modules has been resolved. [DAL-3586]
67. An issue using QXDM with Sierra Wireless cellular modules has been resolved. [DAL-3469]

VERSION 20.5.38.39 (April 2020)

This is a **mandatory** release.

NEW FEATURES

1. LDAP user authentication has been added.
2. An option has been added to the **System > Firmware Update** page to allow the user to update the device from the Digi firmware server.
3. Support for Wi-Fi client isolation has been added. This prevents communication between clients connected to the device's Wi-Fi AP.
4. Support for Digi RM proxy connections has been added.
5. A new **Application** mode has been added for serial ports to allow full control of the serial port by custom Python and Shell scripts. This also allows USB-to-Serial adapters to be access via the /dev/serial/<config-key-name>.

6. Support for the Python HID module has been added.
7. A Digi RM connection watchdog has been added.

ENHANCEMENTS

1. When factory-defaulted, the device will have 2 Wi-Fi Access Points running on 2.4GHz and 5GHz with a SSID of <model>-<serial number> and with the device's default password. The SSIDs and passwords must be configured or the Access Points disabled when configuring the device.
2. The cellular support has been updated to modem PDP context 1 when an AT&T SIM is detected to support new requirements from AT&T.
3. Support for DHCP address pools larger than /24 subnets has been added.
4. Support for AES GCM encryption ciphers has been to IPsec.
5. A new **locally authenticate CLI** option has been added to force a user to login when using the device's CLI via Digi RM.
6. A number of enhancements to the Health Metrics has been made.
    - A new health metric to report the interface being used for an IPsec tunnel has been added.
    - A new health metric to report the LTE SNR has been added.
    - The health metrics have been updated to upload no more than 2 reports per minute if there is a backlog due the connection being down.
    - A debug configuration option to provide a delay window/jitter when uploading the health metrics to Digi RM has been added. The default is 2 minutes.
    - Prevent invalid health metrics data being re-uploaded if Digi RM sends a response that the contents of the health metrics are invalid.
7. The Web UI has been updated so that the **Apply** button on the Device Configuration page is always visible when scrolling down the page.
8. IPv6 support has been added to the **traceroute** command.
9. The Rx and Tx byte count has been added to the **show network interface <name>** command.
10. The OpenVPN server device type connection options have been added to make it easier to select the connection type.
11. A 5 second delay has been added when configuring the LTE band on a Telit modem and rebooting the modem.
12. Support for AT&T LWM2M on the TX54-A146 and TX54-A246 has been added.
13. The network analyzer support has been updated to allow any network interface to be monitored.
14. The idle timeout configuration for remote access serial ports has been updated to be consistent with the user admin idle timeout configuration.
15. The **show system** command has been updated to display the firmware version in the alternate firmware bank.
16. A **broadcast** option has been added to the **ping** command.
17. A **statusall** option has been added to the **show ipsec** command has been added.
18. The Support Report generation has been improved to only run modem AT commands once.
19. Cellular modem firmware files are now retained in the event of the firmware update is

interrupted.

20. The device SKU has been added to the RCI response to Digi RM.
21. The wbdata APN has been added to the APN list.

SECURITY FIXES

14. Updated to openssh-8.2p1 [DAL-2860] CVE-2019-6111 – CVSS Score: 5.8
15. Fixed user escalation exploit through **cloud.drm.sms** configuration option [DAL-2887]
    CVSS Score:6.0 Severity:Medium Matrix: AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
16. Fixed user escalation exploit through **Label** configuration setting for serial ports [DAL-3011]
    CVSS Score: 6.0 Severity: Medium Matrix: AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
17. Fixed password exploit through web token [DAL-3069]
    CVSS Score: 5.6 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N
18. Updated StrongSwan to 5.8.3 [DAL-2866]
19. Updated iputils to s20190709 and traceroute to version 2.1.0 [DAL-2338]
20. Updated Linux kernel to version 5.6 [DAL-2873]
21. Updated ipset to version 7.6 [DAL-2853]
22. Updated OpenSSL to 1.1.1g [DAL-2977] CVE-2020-1967 - CVSS Score – 7.5 HIGH
23. Prevent DOM XSS (cross-site scripting) exploit on **Terminal** page in the web UI [DAL-3068]
    CVSS Score: 4.2 Severity: Medium Matrix: AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
24. Prevent user escalation exploit through netflash options in web UI [DAL-3129]
    CVSS Score: 4.1 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N
25. Prevent use-after-free exploit in CLI configuration of OpenVPN [DAL-2963]
    CVSS Score: 5.7 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N
26. Prevent XSS vulnerability on the **Filesystem** page in the web UI where a directory name with HTML embedded in it would be rendered as HTML rather than plain text [DAL-3200]
    CVSS Score: 4.6 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N
27. Prevent unauthenticated users from downloading the ovpn client configuration file from the web UI [DAL-3133]
    CVSS Score: 5.6 Severity: Medium Matrix: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

BUG FIXES

1. An issue with VRRP crashing on the TX54 has been resolved. [DAL-3181]
2. An IPsec tunnel will now be prevented from being setup if the local network/interface is down. [DAL-2336]
3. Stability issues with the TX64 wifi2 radio have been resolved. [DAL-2359]
4. A Wi-Fi as WAN issue that prevented stale conntrack entries from being flushed when there are network changes. [DAL-2775]
5. An IPsec issue where an IPsec tunnel configured to use a specific interface would not be brought down properly if the interface went down has been resolved. [DAL-3023]
6. An IPsec failover issue which prevent the backup IPsec tunnel found coming up when the primary IPsec tunnel went down has been resolved. [DAL-3024]
7. The analyzer support has been fixed so that it does not stop when the user's SSH connection ends. [DAL-2154]

8. An issue with applying policy based routes to incoming packets from WAN interfaces has been resolved. [DAL-2589]
9. An intermittent reporting issue where the Web UI and CLI would display a modem as registered when it was actually connected has been resolved. [DAL-2329]
10. An issue that prevented IP passthrough mode from working if multicast was also enabled has been resolved. [DAL-2709]
11. An issue with the IPv6 Surelink ping test has been resolved. [DAL-2488]
12. An issue with custom DHCP options not working has been resolved. [DAL-3071]
13. An issue with the **config revert** CLI command has been resolved. [DAL-3194]
14. An issue where a certificate is not received from a SCEP server due to a timing issue between requesting the certificate with a private key and when that certificate can be downloaded has been resolved. [DAL-2850]
15. The Telit module recovery has been improved if a firmware update is interrupted. [DAL-2983, DAL-2984]
16. An issue with the Python **digidevice.led release** function not working correctly has been resolved. [DAL-2566]
17. An issue with inconsistent LED names in the Python **digidevice.led** module has been resolved. [DAL-2569]
18. Issues with TX54 and TX64 WWAN LEDs not behaving correctly have been resolved. [DAL-1045, DAL-2239]
19. An issue with Sierra Wireless RM7511 modem firmware update via the Web UI or shell has been resolved. [DAL-2772, DAL-2773]
20. An issue with the modem firmware on the TX64-A141 which crashed the modem has been resolved. [DAL-2982]
21. An issue with the cellular modem not initializing after the resetting the modem has been resolved. [DAL-1409]
22. An issue preventing the current firmware displayed on the Status > Modems Web UI page for Telit LM940 modems has been resolved. [DAL-2375]
23. An intermittent SIM switching issues with the Telit LM960 modem have been resolved. [DAL-2379, DAL-2495]
24. An error with the **show modem** CLI command when the modem was not connected has been resolved. [DAL-2959]
25. An issue with configuration backups not working if the configuration directory contained files or directory paths longer than 100 characters has been resolved. [DAL-3137]

VERSION 20.2.162.162 (April 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

There are no enhancements in this release.

SECURITY FIXES

There are no security fixes in this release.

BUG FIXES

1. An issue with the switching firmware when switching between SIMs on the Telit LM940 module has been resolved. [DAL-2986]

VERSION 20.2.162.157 (April 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. The firstnet-broadband APN has been added for AT&T FirstNet SIMs.
2. The Rx and Tx byte counts have been added to the **show modem name <name>** command.
3. The MAC address has been added to the support report filename.

SECURITY FIXES

1. Cross-site scripting (XSS) vulnerabilities on the Web UI configuration, status, terminal and file system pages has been resolved. (DAL-2818, DAL-2819, DAL-2823)
2. A script injection exploit on the Web UI Configuration Maintenance has been resolved. (DAL-2797)
3. A fix to prevent unauthorized read/write access to /op/config and /opt/boot when the interactive shell is disabled. (DAL-2865)
4. An issue where the output of the Analyzer could be written out of the /etc/config/analyzer directory has been resolved. (DAL-2672)

BUG FIXES

1. An issue with the Sierra Wireless EM7511 module firmware update has been resolved. (DAL-2794)
2. An issue with the automatic cellular firmware selection on the Telit LM960 modules for T-Mobile and Sprint SIMs has been resolved. (DAL-2376)
3. An issue that was preventing multicast packets from being sent through a network bridge interface has been resolved. (DAL-2774)
4. An issue with the Digi Remote Manager health metrics reporting the /opt directory as full when it wasn't has been resolved. (DAL-2769)
5. An issue where the device would not automatically reboot after restoring configuration using the Web UI has been resolved. (DAL-2862)
6. An issue with the scheduled reboot always using UTC time rather than the configured timezone has been resolved. (DAL-2859)
7. An issue with stopping the analyzer in the CLI has been resolved. (DAL-2892)
8. An issue with the **show system** command on the TX64 when no Bluetooth module has been fitted has been resolved. (DAL-2871)

9. An issue in reading the status of the accelerometer has been resolved. (DAL-2266)

VERSION 20.2.162.90 (March 2020)

This is a **recommended** release.

NEW FEATURES

1. The Connection Monitoring and Active Recovery support has been rebranded as Surelink.
68. The default Surelink settings for WAN interfaces has been changed so that the interface will do DNS tests against its DNS server to determine if the interface is working.
69. Read only admin access has been added.
70. A new shell access parameter has been added to allow you to prevent shell access from being enabled for a group. When disabled, script access to the shell and custom firewall rules are also restricted. If this parameter is subsequently re-enabled, the device will factory-default.
71. Support for TX64 user partition encryption has been added.
72. Support for USB GNSS devices has been added.

ENHANCEMENTS

1. The default setting for 'SIM failover alternative' on Modem interfaces has been changed to 'reset'.
2. Hotspot performance has been improved by reducing the amount of log entries being produced.
3. IPsec status and Tx/Rx byte deltas have been added to the health metrics.
4. HTTPS support has been enabled from the initial boot up.
5. The Web UI has been updated to display devices connected to a hotspot.
6. The IPsec performance on the TX64 has been improved.

SECURITY FIXES

1. The libpcap library has been updated to 1.9.1 (CVE-2017-16808, CVE-2019-15163)
2. The tcpdump application has been updated to 4.9.3 (CVE-2018-14465, CVE-2018-14467 CVE-2018-14470 CVE-2018-14879 CVE-2018-16227 CVE-2018-16452 CVE-2019-15167)
3. The libxml2 library has been update to v2.9.10. (CVE-2018-14567, CVE-2018-9251)
4. The OpenVPN support has been updated to v2.4.4 (CVE-2017-12166)
5. The libldns library has been updated to v1.7.1 (CVE-2017-1000231, CVE-2017-1000232)

BUG FIXES

1. An issue with poor TX54 Wi-Fi client receive speed in bridged configuration has been fixed. (DAL-2353)
2. An issue with the hotspot starting from bootup is has been fixed. (DAL-2446)
3. The health metrics for the TX54 platforms has been fixed. (DAL-2703)
4. The MAC address assignment has been fixed for TX54 and TX64. (DAL-2290)
5. An issue where only the last SSH key configured for a user would work has been fixed. (DAL-2506)
6. An issue with the TX54 (Single Cellular) cellular LEDs has been fixed. (DAL-2659)

7. An issue with the SCEP client handling extra bytes has been fixed. (DAL-2212)
8. An issue with the ping and traceroute commands not routing out of specific interface has been fixed. (DAL-2605)
9. An issue with the TX54 power settings (ignition sense, input voltage, power button behavior) not taking affect has been resolved. (DAL-2734)

VERSION 19.11.72.85 (January 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. The performance for TX54 Wi-Fi client interfaces configured as a bridge has been improved.
2. The MTU is now being displayed with the **show route verbose** CLI command.
3. The Python acl.led module has been moved to the digidevice module.

SECURITY FIXES

There are no security fixes in this release.

BUG FIXES

1. An issue with the Dual APN configuration on the TX54 and TX64 has been resolved. (DAL-2311)
2. An issue with the Active Recovery support on cellular interfaces has been resolved. (DAL-2000)
3. An issue with VLAN support on the TX54 has been resolved. (DAL-2264)
4. An IPsec routing issue when configuring a remote network of 0.0.0.0/0 has been resolved. (DAL-2253)
5. The missing Wi-Fi configuration for the TX54 Dual Wi-Fi variant has been added to support 2.4GHz band. (DAL-2451)
6. An issues enabling the location support for the TX54 platforms has been resolved. (DAL-2226)
7. The MAC address assignment for the TX54 and TX64 Wi-Fi interfaces has been corrected. (DAL-2290)
8. An issue were N/A would be displayed for Network Activity counters on the Web UI dashboard has been resolved. (DAL-2295)

VERSION 19.11.72.53 (December 2019)

The TX54 and TX64 firmware supports the following key features:

- Cellular
    - 4G LTE and 3G support
    - Dual cellular connections

        - SIM prioritization
    - Wi-Fi
        - Access Point support
        - Client support
        - Wi-Fi scanner support
        - Wi-Fi hotspot
    - Digi Remote Manager
        - Remote Management
        - Device Health Metrics
    - VPN
        - IPsec with certificate and pre-shared key authentication
        - HW encryption for IPsec
        - OpenVPN
        - GRE
    - SCEP Client support
    - Web Filtering / Cisco Umbrella
    - Location support
        - On-board GNSS module
        - 3rd party source
        - Forwarding to remote hosts
    - IPv4/IPv6
    - Routing
        - Static Routes
        - Policy based Routing
        - Routing services (BGP, OSPF, RIP, IS-IS)
        - Multicast
    - Port Forwarding
    - Packet Filtering
    - Packet Analyzer
    - IntelliFlow
    - Bluetooth scanner support

The following features from earlier Digi xOS firmware are not yet supported in this DAL beta firmware. They will be supported before in the production release later this year:

- VRRP+ (support added in 20.08.22.32)
- SNMP v1/v2c (support for v2c added in 21.5.56.106)
- SNMP Enterprise MIB
- SSH Certificates
- DMNR (support added in 20.08.22.32)
- DHCP Option User Classes