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

Product Release Notes
Digi WR/LR Product Family
Version 4.8.10 (April, 2021)

INTRODUCTION

These are the release notes for the Digi WR and LR product family of cellular routers.

SUPPORTED PRODUCTS

- Digi WR64
- Digi WR54
- Digi LR54
- Digi LR54W
- Digi LR54-FIPS
- Digi LR54W-FIPS

KNOWN ISSUES

1. With the default WAN configuration, if WAN1 state is configured to be off, the WAN2 (Cellular1-SIM1) interface will not come up. Instead the WAN4 (Cellular1-SIM2) will come up [XOS-1296].
2. On the WR64 and LR54 platforms, Wi-Fi module 1 supports both 2.4GHz and 5GHz bands, it is possible to configure a channel that is outside of the valid range for the band using the CLI (e.g. channel 11 for an AC band). This is not an issue with the Web UI interface [XOS-1267].
3. TransPort WR devices cannot be managed by Digi Remote Manager's Profile Manager if profiles have site-specific settings and custom firewall rules have been configured [TLR-4788].
4. When configuring a WAN interface with 'probe-interval' and 'timeout', the 'probe-interval' must be less than the timeout interval, otherwise the default route may disappear [XOS-250].
5. A fully qualified domain name (FQDN) cannot be used to configure a WAN interface "probe-host" [XOS-2089].
6. A Wi-Fi client interface using WPA2-Personal security cannot connect with a Wi-Fi Access Point using mixed WPA/WPA2 Personal security [XOS-1851].
7. A few configuration and status values reported in DIGI RM can be off by one due to a conversion error. [XOS-1869]
8. The "show ipsec" command may display zero bytes received and transmitted on IPsec tunnels even though data is being transferred through the tunnel.
9. A low cloud keepalive (e.g. 10 seconds) can cause a timeout problem with firmware updates

when done using Digi Remote Manager. The device will be updated but might be reboot once the update is complete.

UPDATE CONSIDERATIONS

UPDATING A LR54 / LR54-FIPS THAT IS RUNNING A PRE-4.3.2 VERSION

If you have a LR54 or LR54-FIPS that is running a pre-4.3.2 version, it must be updated to 4.3.2 before updating to a later release.
To update to 4.3.2

1. Download the firmware update file http://ftp1.digi.com/support/firmware/transport/LR54/v4.3.2.24/lr54-migration-4.3.2.24.bin (or http://ftp1.digi.com/support/firmware/transport/LR54/v4.3.2.24/lr54-fips-migration-4.3.2.24.bin for LR54-FIPS devices) to your PC.
2. In the Web UI, navigate to the System > Firmware Update page.

   In the Getting Started Wizard, navigate through to the Firmware Update page.
3. In the Available Version selection box, select Upload firmware.
4. Click on Choose file and select the downloaded 4.3.2 bin file
5. Click on UPDATE FIRMWARE.
6. Once the LR54 has rebooted, it can be updated to a newer release using the Web UI or Getting Started Wizard which will automatically download the latest release image.

DIFFERENCES BETWEEN 3.2 AND 4.3 RELEASES

Apart from the new features and bug fixes that have been added as part of the 4.0, 4.1 and 4.2 releases which are documented in the History section, there are a few differences between the 3.2 and 4.3 releases.

1. In order to support multiple cellular modules, the **cellular** command has changed. Each **cellular** command instance now maps to a cellular module instead of a SIM. Each instance of the cellular command supports configuration for both SIMs associated with the cellular module.
2. In order to support multiple cellular modules, the **show cellular** command has been updated. The **show cellular** command now supports a summary mode that displays an abbreviated status of the available cellular interfaces. To get the detailed status of a cellular interface, the **show cellular <1|2>** should be used.
3. The **wifi** and **wifi5g** commands have been replaced with the **wifi-ap** command. On the LR54, the **wifi 1 – 4** interfaces have become the **wifi-ap 1 – 4** interfaces and **wifi5g 1 – 4** interfaces have become the **wifi-ap 5 – 8** interfaces.
4. The **show wifi** and **show wifi5g** commands have been replaced by the show wifi-ap command.
5. The **wifi-global** command has been replaced by the **wifi-module** command. The parameters have been updated to better support multiple Wi-Fi modules.
6. The **cellular state** and **wifi state** parameters have been replaced by the **wan state** parameter.
7. The **update modem** command has changed to **update module** command. The remaining parameters for the command are unchanged.
8. The Python version has changed from Python 3.6 to Python 3.5 from the v4.0 release onwards. This was due to a build system change rather than a technical issue with Python 3.6.

As part of the firmware update process, the affected configuration commands and parameters will be automatically updated to the new version in the 4.3 release. You should not have to make any configuration changes due to updating to the 4.3 release.

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update 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, go to https://www.digi.com/products/iot-platform/digi-remote-manager. If you prefer manually updating one device at a time, follow these steps:

1. Log into the Web UI.
2. Navigate to the System > Firmware Update page.
3. Click on the UPDATE FIRMWARE button.
4. The device will automatically reboot once the firmware update is complete.

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, knowledge base 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

VERSION 4.8.10 (April, 2021)

This is a **Mandatory** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. Additional dynamical and static MAC filtering and RSSI threshold filtering options have been added to the Wi-Fi Scanner to reduce the number of Wi-Fi devices being detected.
2. The digidevice Python module has been updated to provide an API to the Wi-Fi Scanner

data.

3. The Python version has been updated to 3.7.8
4. The SCEP client support has been updated to wait up to 5 minutes for a WAN interface to come up before trying to download new certificates.
5. The method how the MTU is set for a carrier's network has been updated to get the MTU from the cellular module.
6. The method how the cellular interfaces statistics are collected has been updated to make the statistics more reactive to changes.

SECURITY FIXES

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

1. Updated DNSMasq to 2.84 [XOS-3719]

   CVE-2020-25681 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 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 5.7 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2020-25684 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 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 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 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

2. Updated OpenSSL to 1.1.1k [XOS-3752]

   CVE-2021-23840 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 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 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 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

3. Updated glibc library to 2.33 [XOS-3733]

   CVE-2019-25013 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2020-27618 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

   CVE-2020-29562 4.8 Medium CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H

   CVE-2021-3326 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2021-27645 2.5 Low CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L

4. Updated libgcrypt to 1.9.2 [XOS-3711]

   CVE-2021-3345 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

5. Updated curl to 7.75 [XOS-3707]

   CVE-2020-8169 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 7.1 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

   CVE-2020-8231 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

   CVE-2020-8284 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

   CVE-2020-8285 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2020-8286 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

6. Updated tcpdump to 4.9.3 and added patch to resolve two vulnerabilities [XOS-3706]

   CVE-2020-8036 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2020-8037 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

7. The hostapd and WPA supplicant packages has been patched to resolve two vulnerabilities [XOS-3705]

   CVE-2019-16275 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 5.9 Medium CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

8. Updated sqlite3 to 3.34.1 [XOS-3697]

   CVE-2020-15358 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2020-13871 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

9. Updated pcre library to 8.44 and pcre2 library to 10.36 [XOS-3734]

   CVE-2020-14155 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

   CVE-2019-20838 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-20454 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

10. Update iproute2 to 5.11.0 [XOS-3773]

    CVE-2019-20795 4.4 Medium CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

11. Updated socat to 1.7.4.1 [XOS-3696]
12. Updated keepalived to 2.2.2 [XOS-3695]
13. The MAC algorithms, ciphers and Diffie-Hellman key exchanges used the SSH server have been updated. [XOS-3754]
14. The cappac application has been updated to resolve a potential buffer overflow. [XOS-3698]
15. The file permissions on some of internal applications have been updated to restrict access. [XOS-3730]

BUG FIXES

1. An issue where the device would display “No buffer space available” messages has been resolved. [XOS-3724]
2. An issue where manually configured DNS servers on cellular interfaces not being used has been resolved. [XOS-3693]
3. An issue where the Hotspot was not working when the web filtering support was also enabled has been resolved. [XOS-3721]
4. An issue when an FQDN was configured for a probe-host over an IPsec tunnel has been resolved. [XOS-3767]
5. An issue with the Wi-Fi client health metrics has been resolved. [XOS-3769]

VERSION 4.8.9 (September, 2020)

This is a **mandatory** release.

For WR54 and WR64 devices using the Telit LM940, Digi recommends that you update to the latest cellular firmware release.

See the Update cellular module firmware section in the User Guide for information on how to do this.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

There are no enhancements in this release.

SECURITY FIXES

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

1. Updated OpenSSL to 1.1.1g [XOS-3625]

   CVE-2019-1543 7.4 High CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

   CVE-2019-1552 3.3 Low CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

   CVE-2019-1547 4.7 Medium CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

   CVE-2019-1549 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

   CVE-2019-1563 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

   CVE-2019-1551 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

2. Updated glibc library to 2.31 [XOS-3622]

   CVE-2018-19591 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-6488 7.8 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2016-10739 5.3 Medium CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

   CVE-2019-7309 5.3 Medium CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-9169 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-19126 3.3 Low CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

3. Updated hostapd to 2.9 [XOS-3624]

   CVE-2017-13082 8.1 High CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

   CVE-2019-9497 8.1 High CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-9498 8.1 High CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-9495 3.7 Low CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

   CVE-2019-9496 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-9494 5.9 Medium CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

4. Updated curl library to 7.69.1 [XOS-3623]

   CVE-2018-16839 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2018-16840 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2018-16842 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

   CVE-2019-3823 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-3822 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2018-16890 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2019-5436 7.8 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-5443 7.8 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-5482 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-5481 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

5. Updated OpenVPN to 2.4.9 [XOS-3673]

   CVE-2020-11810 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

   CVE-2018-9336 7.8 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2018-7544 9.1 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

BUG FIXES

1. The MCU firmware has been updated to correct the power timings of the cellular modules. It will be version 18. [XOS-3645]
2. The cellular module shutdown sequence has been updated to reduce the amount of time it takes for the module to shut down. [WR64-70]
3. An issue with the factory default not deleting the Python history has been resolved. [XOS-3587]
4. An issue with Health Metrics resulting in a message indicating “Failed retrieving Wi-Fi clients” has been resolved. [XOS-3669]

VERSION 4.8.8 (April, 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. The DHCP client on WAN interfaces has been enhanced to include the hostname of the device.
2. The LTE Signal to Noise Ratio (SNR) is now being displayed with the **show cellular <1|2>** command and is also included in the health metrics uploaded to Digi Remote Manager.
3. The health metrics support has been updated to limit the rate at which records are uploaded to Digi Remote Manager (Digi RM) to prevent Digi RM from being overwhelmed if a lot of devices go offline and then reconnect at the same time.

SECURITY FIXES

There are no security fixes in this release.

BUG FIXES

1. An issue with packets being sent out on cellular interfaces with an invalid source IP address which resulted in connections on the Verizon network being dropped has been resolved. (XOS-3594)
2. An issue where an IPsec tunnel with no local subnet configuration could still be established using the WAN interface’s IP address as the local subnet has been resolved. The IPsec tunnel will not be established without a valid local subnet configuration. (XOS-3518)
3. An issue where the cloud connection could get into a hung state if negotiation packets are lost has been resolved. (XOS-3518)
4. An issue with a random IP probe host being set on IPsec tunnels when being configured via the Web UI has been resolved. (XOS-3583)
5. An issue with the device failing to make a new certificate request when a certificate has been revoked by the SCEP server has been resolved. (XOS-3586)
6. An issue with duplicate health metrics being uploaded to Digi RM has been resolved. (XOS-3585)
7. An issue with the Cloud Connector being restarted has been resolved. (XOS-3555)

VERSION 4.8.7 (February, 2020)

This is a **recommended** release.

NEW FEATURES

1. A **show metrics** command has been added to display the status of the health metrics collection and uploading.
2. An **eth-power** command has been added to allow the WR54 and LR54 Ethernet ports to be individually enabled and disabled.
3. A **restart cloud** command has been added to allow the Cloud Connector firmware to be restarted without rebooting the device.

ENHANCEMENTS

1. The **show ipsec-statusall** command has been added that displays the extra status information of the IPsec tunnels.
2. The **show arp** command has been updated so that it does not resolve hostnames. Instead, a question mark will be displayed in the Name column. A new option **show arp hostnames** has been added to allow the IP hostnames to be displayed.
3. The SNTP support has been updated to allow up to three servers to be configured.
4. The Digi RM watchdog has been updated to allow the restart and reboot timeouts to be specifically configured. It has also been updated to use changes in the TCP window size when monitoring the Digi RM connection.
5. The Digi RM health metrics support has been updated so that a random delay of up to 25% of the sample interval will be applied when uploading the health metrics. Previously the random delay had been up to a maximum of 2 minutes.
6. A **clear metrics** command has been added to allow saved metrics to be cleared. (XOS-3504)

SECURITY FIXES

1. The version of Python has been updated to v3.5.9.

BUG FIXES

1. A resource leak when packets are dropped during the initial Digi RM connection handshake has been fixed. (XOS-3534)
2. The Cloud Connector firmware has been updated to use a non-blocking SSL connect and shutdown that could cause a potential hang. (XOS-3531)
3. An issue with IPsec tunnels not being restored after the tunnel goes down has been fixed. (XOS-3503)
4. An issue with duplicate health metrics being uploaded to Digi RM when there is a slow uplink has been fixed. (XOS-3516)
5. An issue where an unusually high IPsec probe latency being reported in the health metrics has been fixed. (XOS-3526)
6. An issue where an IPsec tunnel status was being incorrectly reported as Down in the health metrics. This was due to misreporting when keys were being re-generated. (XOS-3524)
7. An issue with the dhcp-host functionality not working has been fixed. (XOS-3521)
8. An issue with the SCEP client support displaying incorrect error messages has been fixed. (XOS-3506)

VERSION 4.8.6 (January, 2020)

This is a **recommended** release.

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

1. The Digi RM health metrics support has been updated to allow metric groups to be enabled or disabled individually in order to reduce the amount of data being sent. The groups are **all**, **system**, **eth**, **cellular**, **wifi-ap**, **wifi-client**, **location**, **ipsec**, and **power**.
2. The Digi RM health metrics support has been updated to add a short random delay of up to 2 minutes is added to the upload interval so that not all devices are trying to upload at the same time.
3. The IPsec support has been updated add to support to allow the device to be rebooted after a configurable amount of time if an IPsec tunnel cannot be established.
4. The SCEP support has been updated to retrieve a new certificate if the SCEP configuration is changed. SCEP will also delete any existing private key when requesting a new certificate.
5. The SCEP renewal task has been updated to run 4 times a day rather than once a day.
6. The text in the **show system** command for displaying the firmware versions in both banks has been improved.
7. The help text for the **update firmware copy-bank** command has been added.

SECURITY FIXES

1. The Digi RM file hashing algorithm has been updated to use the SHA512 algorithm.

BUG FIXES

1. An issue with the Digi RM support where a DNS request was being sent every 5 minutes has been resolved. (XOS-3493)
2. An issue with the IPsec support where an IPsec tunnel would sometimes not be established has been resolved. (XOS-3461, XOS-3486)
3. An issue with the SCEP certificate renewal has been resolved. (XOS-3491)
4. An issue that was preventing the received CA certificate from being accepted if there were additional bytes in the SCEP message have been resolved. (XOS-3429)

VERSION 4.8.4 (October, 2019)

This is a **recommended** release.

NEW FEATURES

1. A new CLI command, **update firmware copy-bank** has been added to allow the user to copy the current running firmware version into the other firmware bank.
2. A new CLI command, **update firmware switch**, has been added to allow the user to switch firmware banks.

ENHANCEMENTS

1. The WAN failover support has been updated so that the device will not be rebooted if there is a higher priority WAN interface already up.

SECURITY FIXES

There are no security fixes in this release.

BUG FIXES

1. An issue with IPsec tunnels configured with a remote subnet of 0.0.0.0/0 having problems with local LAN traffic such as DHCP has been resolved. (XOS-3380)
2. An issue with configuring password parameters over a length greater than 15 characters has been resolved. (XOS-3400)
3. An issue with the **show vrrp** command has been resolved when a probe gateway is not configured and the device is using a cellular WAN interface. (XOS-3409)

VERSION 4.8.1 (August, 2019)

This is a **recommended** release.

NEW FEATURES

1. Spanning Tree Protocol (STP) support has been added to LAN interfaces.

BUG FIXES

1. A WR54 and LR54 flash driver issue that could result in the configuration being lost and the device factory defaulting has been resolved. (XOS-3211)

VERSION 4.8.0 (August, 2019)

This is a **recommended** release.

NEW FEATURES

1. IPsec certificate authentication support, including support for chained certificates, has been added.
2. Support for IPsec to failover to a backup tunnel has been added.
3. SCEP client support has been added to allow for the automatic updating of PEM format certificates and certificate revocation lists (CRLs).
4. Support for a performance (iperf3) server that allows the user to test the performance of networks has been added.
5. Support for a Wi-Fi scanner that allows the device to report what Wi-Fi devices are close by has been added.
6. Support for a Bluetooth scanner that allows the device to report what Bluetooth (BLE) devices are close by has been added.
7. Support to allow the GNSS module to be used as a time source for the NTP server support has been added.
8. Support for EAP-TLS certificate authentication for WPA-Enterprise security when in Wi-Fi client mode has been added.
9. Support for Python Digi RM callbacks has been added.
10. Support for clearing the DHCP server cache has been added.
11. Support has been added the WR64 to enable an auto-reboot mode if the input voltage temporarily drops low enough to cause the WR64 to power down.

ENHANCEMENTS

1. The version of Python supported has been updated to 3.5.7.

2. The “TransPort” branding has been dropped. Apart from the visual Web UI differences, the only other difference is the module name in the Enterprise MIB which has changed. The OIDs in the MIB are still the same.

SECURITY FIXES

1. The patches for the TCP SACK Panic vulnerabilities have been applied. (CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479)
2. HSTS support has been added to the Web server.

BUG FIXES

1. An issue with IPsec when using IPv4 addresses as local and remote IDs has been resolved.
2. The output of the “update module show” command has been fixed.
3. An issue with some of the IPsec tunnel metrics not be reported to Digi RM has been resolved.

VERSION 4.7.0 (May, 2019)

Initial WR54 Dual Wi-Fi production release.

VERSION 4.6.1 (April, 2019)

This is a **recommended** release.

SECURITY FIXES

1. A number of security fixes have been made to resolve command injection and buffer overflows exploits via the CLI, Web sockets and SNMP. The rating of these exploits are medium to high level and authenticated admin access to the device is required for all of the exploits.

VERSION 4.6.0 (March, 2019)

NEW FEATURES

1. Support for IPsec Failover has been added. The device will automatically renegotiate the IPsec tunnel using an alternative WAN interface if it detects the WAN interface it had been using has gone down.
2. Support for IPsec probing has been added. This allows the device to send probe packets through the IPsec tunnel and to renegotiate it if there are no probe responses for a configured period of time.
3. Support for Digi’s VRRP+ has been added. This allows a VRRP backup device to monitor the VRRP master and to promote itself if a problem is detected.
4. Commands have been added to display and clear the ARP table.
5. Support for OpenVPN TLS Authentication has been added.
6. Support for USB Serial adapters has been added. Devices using the prolific or FTDI chipsets are supported.

ENHANCEMENTS

1. The Digi Remote Manager (Digi RM) health metrics support has been updated to support a configurable rollup period. The rollup period is the amount of time the health metrics are aggregated before being reported to Digi RM. It is recommended that the health metrics sample and rollup periods are set to the same value.
   By default, health configurations on Digi RM use 1 hour rollup periods. For example, a system uptime of 3600 seconds is considered normal for a 1 hour period. If you are using health profiles, change the health profile settings on Digi RM when changing the rollup period to avoid false health alarms. For example, if changing the rollup period to 5 minutes, the system uptime rule would use 300 seconds for normal uptime.
2. The DMNR support has been updated to support a configurable reconnection timer.
3. An **IPsec configuration has been added to force an IPsec tunnel to use NAT-T UDP encapsulation**.
4. The port forwarding source interface configuration now supports GRE and OpenVPN client interfaces.
5. The Python digidevice module has been updated to support a LED library to allow the device's LEDs to be controlled by Python applications.

BUG FIXES

1. An issue where IPsec ESP packets being incorrectly sent on a cellular WAN interface after failing over from an Ethernet WAN has been resolved. Depending on the carrier, this could result in being disconnected from the cellular network. (XOS-2974)
2. An issue with WAN SIM to SIM failover where it would not switch to the lower priority WAN interface if the higher priority WAN interface is still not operational has been resolved. (XOS-2868)
3. An issue with OpenVPN where static routes would not be reinstalled after an OpenVPN interface has gone down and then back up again has been resolved. (XOS-2964)
4. The "show ipsec" command has been updated to resolve a number of issues that could result in an error response. (XOS-2371)
5. An issue with IPsec ESP authentication SHA384 algorithm on the WR64 has been resolved. (XOS-2915)
6. An issue with the WR54 ignition sense support where the device would not power up after the configured delay once the ignition sense line goes high has been resolved. (XOS-3021)
7. An issue with location prefix being concatenated on second and subsequent data streams has been resolved. (XOS-2988)
8. The missing serial baud rate parameter has been added to the Web UI. (XOS-2865)

VERSION 4.5.2 (WR64) (January, 2019)

VERSION 4.5.1 (WR54, LR54) (December, 2018)

NEW FEATURES

1. PySerial support for the Serial interface has been added.
2. Support for DHCP static IP address assignment has been added.
3. Support for DHCP options including user-class support has been added.

ENHANCEMENTS

1. DMNR support has been updated so that it will automatically reconnect if the connection is dropped or rejected.

SECURITY FIXES

1. A major security issue has been resolved. See CVE-2018-20162 for more information.

BUG FIXES

1. An issue with SIM PIN support has been resolved. (XOS-2791)
2. A Digi Remote Manager connection issue when using Wi-Fi client interfaces has been resolved. (XOS-2771)
3. An issue with forwarded TAIP messages with replaced vehicle IDs containing additional data has been resolved. (XOS-2752)
4. An issue with the WR64 where is could continually reboot at 2.5 minutes has been resolved. (XOS-2897)

VERSION 4.5.0 (December, 2018)

Initial WR54 Firstnet production release.

VERSION 4.4.0 (October, 2018)

NEW FEATURES

1. Support for an NTP server has been added.

ENHANCEMENTS

1. IPsec support has been updated to add the following functionality:
    a. IKEv2
    b. Multiple IP subnet support
    c. SHA384 authentication for ESP and IKE (WR64 only)
    d. AES GCM encryption for ESP and IKE (WR64 only)
    e. Diffie-Hellman group 20 for ESP and IKE
    f. Xauth authentication for client and server modes
    g. IPsec debug now supports levels -1 to 4 to give better granularity and information when diagnosing IPsec issues
2. The location support on the WR64 has been updated to add the following functionality:
    a. Accept NMEA and TAIP messages from an external device over UDP.
    b. Forward NMEA and TAIP messages to external devices over UDP.
    c. The **location gnss-state <on| off>** command has been changed to the **location state <off | gnss | server>** to support the new location server functionality. The default is still to enable the GNSS module. Any existing location configuration will automatically be converted to the new command.

BUG FIXES

1. An issue with the DHCP server messages being incorrectly routed when there is an IPsec tunnel with a remote subnet of 0.0.0.0/0 has been resolved. [XOS-2194]
2. A VRRP issue where an LR54 could become the master even if there were higher priority device already a master has been resolved. [XOS-2402]
3. An issue when configuring a LAN IP address and DHCP server parameters which could leave the DHCP giving out old gateway and DNS server information has been resolved. [XOS-1952]
4. The traffic analyzer support has been updated to correct decode GRE headers. [XOS-1141]

VERSION 4.3.2 (September, 2018)

NEW FEATURES

1. Support for IPv6 on the WAN and LAN interfaces has been added.
2. Support for SIM PINs has been added.
3. Support for DMNR has been added.
4. Support for GRE has been added.
5. Support for OpenVPN client compression has been added.
6. Support for configuration static routes over OpenVPN interfaces has been added.

ENHANCEMENTS

1. Support for the Digi TransPort LR54, LR54W, LR54-FIPS and LR54W-FIPS platforms.
   This is the first update to the LR54, LR54W, LR54-FIPS and LR54W-FIPS platforms since the 3.2.2 release.

   If you are running an earlier version than 3.2.2, we recommend that you reboot your device and update to the 3.2.2 release first, before updating to 4.3.2 afterwards.

   To update to 3.2.2:

   1. Download the firmware update file http://ftp1.digi.com/support/firmware/transport/LR54/v3.2.2.1/lr54-3.2.2.1.bin (or http://ftp1.digi.com/support/firmware/transport/LR54/v3.2.2.1/lr54-fips-3.2.2.1.bin for LR54-FIPS devices) to your PC.
   2. In the Web UI, navigate to the System > Firmware Update page.
      In the Getting Started Wizard, navigate through to the Firmware Update page.
   3. In the **Available Version** selection box, select **Upload firmware**.
   4. Click on **Choose file** and select the downloaded 3.2.2.1 bin file
   5. Click on **UPDATE FIRMWARE**.

   The firmware update from 3.2.2 to 4.3.2 will take approx. 3 minutes 40 seconds. If you are doing the firmware update via the Web UI or Getting Started Wizard, you may see the Web UI or Getting Started Wizard timeout as it waits for the LR54 to reboot. The Web UI or Getting Started Wizard may automatically reconnect once the LR54 has rebooted, or you may have to manually reconnect.

   Note: Once the LR54 device has been updated to v4.3.2, it cannot be downgraded to an earlier release.

BUG FIXES

1. The system time and timezone support has been updated to ensure that they are set together during bootup. [XOS-2353]
2. An issue with the LR54 HW crypto support that resulted in IPsec packets of certain sizes being dropped when received over cellular interfaces has been resolved. [XOS-2225]
3. The IPsec support has been updated to ensure a route added for an IPsec tunnel is correctly removed when the tunnel does down. [XOS-2303]

VERSION 4.2.1 (May, 2018)

NEW FEATURES

1. Support for policy based routing has been added.

ENHANCEMENTS

1. Surelink has been updated to support the resetting of the cellular module and the router when probing fails.

BUG FIXES

1. A hotspot issue where data could not be sent over Wi-Fi client WAN interfaces has been resolved. [XOS-1926]
2. An issue when changing the LAN IP address using the Web UI changing the DHCP server settings has been resolved. [XOS-1952]
3. A syntax error in the geo-tagging of the Health Metrics messages when there is no fix has been resolved. [XOS-1871]
4. An issue with the drop down menus on the Port Forwarding Web UI page has been resolved. [XOS-1881]

VERSION 4.2.0 (April, 2018)

ENHANCEMENTS

1. Wi-Fi as WAN support has been added. The WR64 supports up to two active Wi-Fi WAN interfaces at once (one on each Wi-Fi module) although you can configure up to 16 Wi-Fi networks which can be assigned to one of the Wi-Fi WAN interfaces. The Wi-Fi WAN interface will scan through the assigned networks and connect to one that it finds.
2. The Health Metrics support has been updated to include Wi-Fi as WAN metrics, location tagging and configurable sampling periods.
3. Support for the Hotspotsystem.com service has been added.
4. A configurable cellular registration timeout has been added so that the cellular module will be reset if it cannot register with a network.
5. The WR64 can now be configured to disable the power button from powering down the device.
6. The gps command has been changed to be location to make it more extensible in the future.

BUG FIXES

1. A WAN failover probing issue where a device could switch back to a WAN interface without the probing being successful has been fixed [XOS-1294].

2. A WAN failover issue on a second cellular module where the device could not switch back to SIM1 after failing over to SIM2 has been fixed [XOS-1389].
3. An issue where Wi-Fi interfaces would remain active after being removed from a LAN interface has been fixed [XOS-1136].
4. The WAN probing issue where a reboot was required after changing the probe host has been fixed [XOS-356].
5. An issue with the hotspot support where the upstream and downstream bandwidth was being incorrectly throttled has been fixed [XOS-1521].
6. An issue where a SNMP walk of the Enterprise MIB would fail has been fixed [XOS-1677].
7. A memory error when using the help utility in the Python interactive has been fixed [XOS-1669].
8. An issue where an interface could be assigned to multiple WAN interfaces has been fixed [XOS-242].
9. An issue where the location GNSS state could spuriously turn off and on has been fixed [XOS-1415].

VERSION 4.1.0 (February, 2018)

ENHANCEMENTS

1. Wi-Fi Hotspot functionality
2. TLR functionality

VERSION 4.0.0 (December, 2017)

Initial WR64 production release.