Wireless Vehicle Adapter Release Notes
Version 3.4.0.26 (September 28, 2020)

INTRODUCTION

The Wireless Vehicle Bus Adapter (WVA) is a basic fleet component that makes vehicle bus data, in either J1939/CAN or J1587/J1708 form, available via wireless communication. The Adapter is low-cost and simple to install. It can be used in a desktop development environment with a CAN bus simulator, and can be mounted in a vehicle by plugging into the CAN bus connector. The WVA acts as a Wi-Fi Client connecting to a Wi-Fi-enabled Internet-connected hotspot in the desktop development environment or the vehicle. It is part of a larger system, including a smart phone, tablet, or other on-board computer (OBC), where the developer or vehicle driver can interact with the data provided by the WVA through Wi-Fi.

SUPPORTED PRODUCTS

- WVA-J200
- WVA-J300

KNOWN ISSUES

None

UPDATE CONSIDERATIONS

The power management feature for waking on movement has been removed from this version.

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. Configuration
   c. 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 using the web interface you can find instructions for using the web interface here:
https://www.digi.com/resources/documentation/digidocs/90001929/default.htm#Task/T_config_o

pen_webui.htm.

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

VERSION 3.4.0.26 (September 28, 2020)

This is a **mandatory** release.

NEW FEATURES

1. Added Wi-Fi watchdog feature.
2. Add WLAN diagnostics to detect issues with loading Wi-Fi driver.
3. Added detailed source information such which CAN bus, the protocol used to obtain the data, source address, PGN, SPN, units for the value, more accurate sample timestamp, for each data point collected.
4. Added optional heartbeat message on event channel as well as event channel status endpoint.

ENHANCEMENTS

1. Updated CAN driver.
2. Improved auto-baud mechanism.
3. Improved VIN collection.
4. Improved log organization to avoid rapid log wrapping.
    -   Added vbusd.log for vehicle bus related messages with a max size of 1 MB.
    -   Added cherokee.log for tracking web server activity with a max size of 500 KB.
    -   Redirected some messages from WPA supplicant into wifi.log and increased its size from 500 KB to 1 MB.
    -   Redirected some messages generated during a boot up to kernel.log.
    -   Increased digi.log max size from 500 KB to 1MB.
5. Updated to v1.1.4 of Noregon's vehicle data bus interface library (DBI).
    -   This included an improved default configuration file with additional sources for various data items.
    -   Increased the number of filters in a filter group from eight to 100.
    -   Other miscellaneous bug fixes and improvements.

SECURITY FIXES

1. Dropbear Security Issues (CVE-2016-7406, CVE-2016-7407, -2016-7408, CVE-2017-9078)
2. Addressed potential privilege escalation vulnerabilities.

BUG FIXES

1. Fixed J1708 stale data issue. This resulted in the removal of the wake on movement feature.
2. Added U-Boot verify flag to avoid switching partitions during sub-optimal power conditions.
3. Resolved Wi-Fi Direct periodic disconnect.

VERSION 3.2.25.10 (January 03, 2017)

NEW FEATURES

ENHANCEMENTS

SECURITY FIXES

1. WVA-1740 - Fix WVA KRACK security issue
2. Update firmware to fix a security issue with Wi-Fi.
3. WPA 2 Security issue (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088.)

BUG FIXES

VERSION 3.2.25.9 (January 16, 2017)

NEW FEATURES

1. WVA-1695 - Add new web services endpoint for J1708/J1587 engine VIN at /ws/vehicle/ecus/mid128/VIN; query bus and populate endpoint when engine detected.

ENHANCEMENTS

1. WVA-1697 - Implemented issue detection and recovery in the unlikely case that the Wi-Fi module were to stop responding.
2. WVA-1694 - Wi-Fi device driver specific messages are now directed to a new, dedicated location: "wifi.log"

SECURITY FIXES

1. WVA-1740 - Fix WVA KRACK security issue
2. Update firmware to fix a security issue with Wi-Fi.
3. WPA 2 Security issue (CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088.)

BUG FIXES

1. WVA-1689 - Updated Wi-Fi firmware to improve reliability.
2. WVA-1688 - Fixed J1708 transmission issue preventing J1708 requests from being serviced.
3. WVA-1661 - Improved reliability of J1708 and device power controller.

VERSION 3.2.25.6 (July 14, 2016)

NEW FEATURES

1. For the convenience of customers using the WVA to gather data related to Hours of Service (HOS) logging, two new data points have been added. These data points prioritize distance reporting from the engine, from either the J1587 or J1939 bus, and expose it as TotalDistance_HOS (reporting in km) and TotalDistanceMiles_HOS (reporting in miles).
2. WVA-1587 Create new vehicle data points for Vehicle Speed, Total Distance, and Hi-Res Total Distance that match specific vehicle ECU addresses. For instance, TotalDistance_0 will capture any Total Distance reading for J1939 ECU source address 0, whereas TotalDistance_J1587_128 will capture Total Distance readings generated by MID 128 on the J1587 bus.

ENHANCEMENTS

SECURITY FIXES

BUG FIXES

VERSION 3.2.25.2, 3.2.25.3 (February 24, 2016)

NEW FEATURES
1. Support for WVA-J500 hardware is now present. Due to the differences in hardware, the WVA-J200 and WVA-J500 devices have unique firmware images.
1. Support for the configuration of multiple unique infrastructure networks has been added. Networks can be added to the known list via RCI as well as an enhanced web wizard.
2. Web Service subscriptions can now be registered against endpoints in the /ws/config tree.

ENHANCEMENTS

SECURITY FIXES
1. OpenSSL has been updated from version 'm' to version 'p', addressing the following vulnerabilities: CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792

BUG FIXES
1. OpenSSL header compression has been disabled to avoid the CRIME man-in-the-middle vulnerability.
2. OpenSSL/TLS support in the web server is NOW limited to TLS v1.2 to avoid "BEAST" OpenSSL vulnerability.
3. WVA-1389 - Change infrastructure network scanning method to prevent intermittent outage of WVA access point.
4. WVA-1398 - Fix initial state of DHCP checkbox in Wi-Fi access point configuration web page.
5. WVA-1344 - Fix HiResTotalDistance on second CAN bus.
6. WVA-1393 - Address frozen CAN bus triggered by repeatedly disconnecting and reconnecting CAN simulator.
7. WVA-1391 - Change ECU detection method to address vehicles that do not respond to standard J1939 address query.
8. WVA-1379 - Improve VIN handling by preventing periodic loss of VIN while updating list of attached vehicle ECUs.

VERSION 3.2.15.3 (July 24, 2015)

NEW FEATURES

1. WVA-1301 - Allow configuration of time through the Web UI manually or via NTP
2. WVA-1302 - Allow loading of custom vehicle data configuration files into device
3. WVA-1304 - Allow subscriptions to be set at a minimum of 100ms interval

ENHANCEMENTS

SECURITY FIXES

BUG FIXES

1. WVA-1305 - In some cases configured alarms were not enabled
2. WVA-1307 - Current DTC detection mechanism does not work if ECU is powered off
3. WVA-1377 - Reported Vehicle Speed values can be in error when truck is stopped

VERSION 3.2.10.4 (October 12, 2014)

NEW FEATURES

1. Added support for Wi-Fi Direct
2. Add support for execution of custom python scripts
3. Add support for hardware acceleration information via python script
4. WVA-765 - Add support for J1939 Diagnostic Trouble Codes
5. WVA-953 - Python programmability in WVA
6. WVA-954 - Add CAN statistics to RCI / Web Services
7. WVA-1078 - Add support for hardware acceleration information via python script
8. WVA-1174 - Add support for Wi-Fi direct settings via python script

ENHANCEMENTS

1. WVA-871 - Extend alarms and subscriptions to support DTC
2. WVA-886 - Increase number of queued Subscription/Alarm messages to 20,000

SECURITY FIXES

BUG FIXES

1. WVA-717 - LED text in web UI When configuring the WVA to work with a new AP, after hitting save a message pops up that states the following, "Examine the LEDs to determine whether the device successfully connects to the wireless network." The WVA does not have an LED to indicate network connection so this text was removed.
2. WVA-959 - Web services returning wrong response when using JSON for CAN bus statistics
3. WVA-963 - Web services returns lists with incorrect top level element name
4. WVA-972 - WVA occasionally stops detecting J1587 messages

VERSION 3.2.8.4 (July 29, 2014)

NEW FEATURES

1. WVA-765 - Expose J1939 Diagnostic Codes via Web Services
2. WVA-913 - Add CAN statistics to Web UI
3. WVA-954 - Add CAN statistics Web Services
4. WVA-886 - Increase number of queued Subscription/Alarm messages to 20,000
5. WVA-953 - Python programmability

ENHANCEMENTS

SECURITY FIXES

BUG FIXES
1. WVA-717 - LED text in web UI was removed

VERSION 3.2.1.34 (April 16, 2014)

NEW FEATURES

ENHANCEMENTS

SECURITY FIXES
1. Remove SSL HeartBeat extension from OpenSSL library (HeartBleed workaround for OpenSSL CVE-2014-0160)
2. DBL-624 - Update OpenSSL to resolve the 'heartbleed' vulnerability

BUG FIXES

VERSION 3.2.1.33 (April 16, 2014)

NEW FEATURES
1. Pilot Release

ENHANCEMENTS

SECURITY FIXES
2. Remove SSL HeartBeat extension from OpenSSL library (HeartBleed workaround for OpenSSL CVE-2014-0160)
3. DBL-624 - Update OpenSSL to resolve the 'heartbleed' vulnerability

BUG FIXES