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

Firmware Release Notes
AnywhereUSB Gen 2
Version 2.02 (April 21, 2020)

INTRODUCTION

This is a production release of the AnywhereUSB Generation 2 firmware.

SUPPORTED PRODUCTS

- AnywhereUSB/2
- AnywhereUSB/5
- AnywhereUSB/5 MHC
- AnywhereUSB/14
- AnywhereUSB/TS44

KNOWN ISSUES

Although AnywhereUSB lets you install multiple identity certificates we recommend you only install a single certificate.

AnywhereUSB DOES NOT let you install SSL certificate chains. Only an end-user certificate can be installed on AnywhereUSB. This means that the trusted certificate authority (CA) should directly sign the end-user certificate.

There is a compatibility issue with the Belkin USB 2.0 4-port mobile powered hub model F5U404BLK. The AnywhereUSB will assert (crash) if you physically disconnect it from one of its ports while it is connected to a client PC. We plan to fix this in a future release.

If you upgrade to this version or rev M1 from an older version there is a possibility that when you install (upload) an SSL certificate from the Web UI it will not persist across a reboot. If this happens, you will see a 1024-bit RSA certificate highlighted in red indicating "No matching certificate found". You can work around this issue by restoring factory defaults and re-installing the SSL certificate. The SSL certificate is installed from http://[host]/admin/certificate_management/ssl_tls_identity.htm.

UPDATE CONSIDERATIONS

In order to add compliance with California's Senate Bill No. 327, for information privacy of connected devices, the handling of the root password for newly manufactured products is changing.

Products manufactured after January 1, 2020 will no longer use a fixed, default root password. Rather, a per-device, unique password will be assigned during manufacturing, and will be visible on a product label. It will still be possible to change the password for the root user on a per-device basis.

Products manufactured prior to the adoption of the new product labeling are grandfathered in and will continue to operate as before, with the following exception:

- AnywhereUSB products manufactured before January 1, 2020, which currently do not have passwords set on them, will have a new default password of "dbps" after upgrading to this firmware. The respective username is "root". THIS NEW DEFAULT PASSWORD SHOULD BE CHANGED, this may be done via the web UI by navigating to Configuration – Security.

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. Firmware update process

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, and knowledge base and peer-to-peer support forums. Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 2.02 April 21, 2020 (T)

This is a mandatory release.

ENHANCEMENTS

- The ability to enable SNMP traps to indicate changes in the state of Ethernet link have been added to the product, including the web and CLI user interfaces.

SECURITY FIXES

- Researchers from JSOF (https://jsof-tech.com/), have found vulnerabilities within in the Treck TCP/IP, IPv4, IPv6, DHCP, DHCPv6 and DNS products.

For Digi products we have rated the vulnerabilities as a high level risk. We recommend that customers immediately review and deploy the latest firmware associated with this release note to protect their devices. At time of release of this firmware, there is no known in the wild exploit of these vulnerabilities.

Digi's internal scoring of the vulnerabilities is a CVSSv3.0 Score of 7.4.
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Digi will be coordinating a public disclosure of the vulnerabilities with JSOF that is tentatively set for May 14th, 2020. We are also working with the Cert Coordination Center and have been assigned VU#257161 pertaining to these issues.

Many thanks to the researchers Moshe Kol and Shlomi Oberman of JSOF for reporting these vulnerabilities.

BUG FIXES

None.

VERSION 2.01 November 20, 2019 (S)

This is a mandatory release.

NEW FEATURES

Added support for California's Senate Bill No. 327. Product manufactured after January 1, 2020 will have a unique password.

ENHANCEMENTS

None

SECURITY FIXES

Researchers have discovered new denial-of-service (DoS) vulnerabilities in Linux and FreeBSD kernels, including a severe vulnerability called SACK Panic that could allow malicious actors to remotely crash servers and disrupt communications, according to an advisory.

"The vulnerabilities specifically relate to the Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic," allows a remotely-triggered kernel panic on recent Linux kernels," the advisory stated. This vulnerability also goes back a long time (since Linux v2.6.29, that was released 10 years ago).

"The issues have been assigned multiple CVEs: CVE-2019-11477 is considered an Important severity, whereas CVE-2019-11478 and CVE-2019-11479 are considered a Moderate severity".

BUG FIXES

There was a small memory leak which happens when a secure SSL connection is established.

VERSION 1.97 (R1)

- There is a very small memory leak which happens at the beginning of each AnywhereUSB connection. This usually only has an effect if hosts are competing for a Group that is already in use. This could eventually cause the AnywhereUSB hub to go offline and require a power

cycle to recover.

- The default Duplex Mode for the Ethernet Interface (found in Network Configuration / Advanced Network Settings) has been changed from Half-Duplex to Full-Duplex. This may not take effect if you upgrade from an earlier firmware release. This was fixed back in 1.60 rev F but reappeared in a subsequent release.
- AnywhereUSB/14 only. The current network failover status displays the gateway address backwards. Fixed.
- The byte order in self-signed certificate CN field was reversed. Fixed.

VERSION 1.96 (R)

- This release contains a new TLS implementation
- We now support many more modern and secure cipher suite options as well. This release provides added support for elliptic curve encryption, more hash algorithms, and block modes.
- Support for DSA keys and DSA signed certificates has been removed
- Some places where MD5 was being used as a hash have been modified to no longer use MD5 as it has been compromised. For legacy compatibility most places will still allow MD5 but users are encouraged to change this to something more secure.
- Certificates and certificate requests generated by the product will now be signed with a SHA256 hash.

VERSION 1.95 (P)

- *Power off port when relinquishing ownership of a group instead of disabling the port (AWUSB-501).
- TCP port for Encrypted Realport was incorrectly saved for the Encrypted AnywhereUSB TCP Port. Fixed. (AWUSB-470)
- Disable TLS 1.0 for all secure connections. (AWUSB-424)
- Only use SHA-256 for self-generated cert. (AWUSB-525)
- When a user uploaded an identity certificate and private key pair, the TLS server mistakenly used the self-generated key with the user-supplied certificate instead of the user-supplied key (AWUSB-434). Fixed.

* Only affects AnywhereUSB/14 and AnywhereUSB/5m which support Dynamic Group Assignment.

VERSION 1.93

Rev N1 (v1.93.21)

- TLS v1.2 and SHA-2 (SHA-256) support.

- AnywhereUSB now supports TLS v1.2 "Encrypted AnywhereUSB" connections and HTTPS connections. Along with this, AnywhereUSB also supports SHA-2 (SHA-256) certificates as well as SHA-1 certificates. This means web browsers which require TLS 1.2 servers (that is, they no longer fallback to TLS 1.0or TLS 1.1) can still use the secure HTTPS protocol with AnywhereUSB's web server. It also means that customers may use SHA-2 certificates as well as SHA-1 certificates to authenticate "Encrypted AnywhereUSB" connections.

NOTE: TLS v1.2 support for "Encrypted AnywhereUSB" connections requires an upgrade to driver Rev P (v3.90.223).

VERSION 1.92

Rev M1 (v1.92.2003)

- [NDS-575 / AWUSB-381] This AnywhereUSB device has a critical vulnerability: CVE-2014-9222. Fixed.
- [NDS-574 / AWUSB-381] This AnywhereUSB device has a related critical vulnerability: CVE-2014-9223. Fixed.
- [AWUSB-390] Rare exception occurred related to network outages. Fixed.

VERSION 1.90

Rev M (v1.90.1855)

- Remote Management (previously known as Device Cloud) support. A user can now remotely manage AnywhereUSB via my.devicecloud.com.See User's Guide for details.

VERSION 1.84

Rev L4 (v1.84.1764)

- Add 10ms delay between resetting device and setting its address to get it to work with FTDI USB to Serial converters.

VERSION 1.83

Rev L3 (v1.83.1732)

- Latest version of Chrome (45) fails with an error code of ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION when you try to open a a secure WebUI connection with an AnywhereUSB hub because of a bug in TLS v1.0. Fixed. JIRA AWUSB-274.
- Disable TCP Port fields for AnywhereUSB and Encrypted AnywhereUSB services since they are not configurable. JIRA AWUSB-275.

VERSION 1.82

Rev L2 (v1.82.1646)

- Enhanced RealportUSB settings interface in CLI so that multiple ports can be configured for a group. JIRA AWUSB-208.

VERSION 1.81

Rev L1 (v1.81.1569)

- -Inbound USB transfers over an encrypted connection which were larger than 1024 bytes were corrupted. Fixed.
- On an encrypted connection AnywhereUSB reported the IP address of the "owned by" host computer incorrectly as the local host IP address of 127.0.0.1. The AnywhereUSB Configuration Utility would display this incorrectly. It has been fixed.

VERSION 1.80

Rev L (v1.80.1545)

- Remove SSL v3.0 support in order to defend against Poodle Attack.
- Tunneling support so that all traffic between a host computer and the AnywhereUSB goes over a single connection instead of multiple connections. This substantially reduces enumeration latencies. This requires AnywhereUSB driver v3.70 and up. Refer to driver release notes.

VERSION 1.70

Rev K1 (v1.70.1475)

- Fix possible race condition which could lead to a device lockup in a condition with many port connection changes.
- Fix an exception that happened if the AnywhereUSB lost its host connection during a device enumeration.
- An exception could occur with many devices because of resource exhaustion. This was a false positive and has been fixed.
- -Backups (backup.cfg) were corrupted. Fixed.

- Add Dynamic Group Assignment(DGA) feature which lets an administrator change Group assignments on the fly without requiring a reboot of the AnywhereUSB. This means there will be no disruption to unaffected ports.
- Check the "Enable Dynamic Group Assignment" box in the Realport USB section of the Web UI and reboot the AnywhereUSB.

Note -

- Default Group is being deprecated and can no longer be edited in the Web UI. Default Group is now "1" and cannot be changed. Host computers must now be configured with specific Group numbers.

VERSION 1.60

Rev K (v1.60.1421)

- Port 5 now supports Low and Full Speed devices as well as High Speed Devices
- Fix two bugs that led to exceptions and/or BSODs when errors occur during device enumeration.
- Workaround for IRP mapping to recover in case a sequence number never comes in.
- Configurable exception handling. From the CLI, the user can specify how the AnywhereUSB behaves if and when an exception happens.

There are 3 Behaviors which can be selected:

1. Blink LEDs. This is the original behavior. When this happens, the user must press the front panel button to reset the unit or put it in crashdump upload mode.
2. Reset. This is now the new default behavior. If and when an exception happens, the unit will reboot itself and preserve the panic record so that it may be displayed from the CLI.
3. Crashdump Mode. If and when an exception happens, the unit automatically goes into crashdump mode so that a user can upload the crashdump from a TFTP client.

For help, type "help set exception" from the CLI.

- Firmware support for encrypted Anywhere/USB traffic. This requires a new client driver which has not yet been released.
- The default Duplex Mode for the Ethernet Interface (found in Network Configuration / Advanced Network Settings) has been changed from Half-Duplex to Full-Duplex. This may not take effect if you upgrade from an earlier firmware release.

VERSION 1.51

Rev F (1.51.1220)

- Support for High Speed USB devices at actual High Speed link speed. Users should not expect performance like that of a directly attached USB connection since the Ethernet adapter is limited to is 100 MB/s . For example, it takes 234 seconds to read a 1Gb file from a USB flash drive connected to the AnywhereUSB/14. It only takes 60 seconds for a USB flash

drive connected directly to a PC USB port. However, that is a big improvement from previous firmware which takes 1175 seconds. This firmware is incompatible with Windows driver releases prior to v3.51.

- Added TFTP support for uploading crash dumps. Crash dumps can no longer be uploaded via serial ports. TFTP is simpler and supported across entire product line instead of just those with serial ports.
- Enabled TCP ACK PUSH option to expedite URB cancellations. This sped up the removal of the Rhode Scwarz NRPZ-31 Power Sensor which queues many URBs during normal operation.
- During device enumeration if Select Configuration failed, the firmware would still try to use the returned NULL pipe handle(s) leading to an ASSERT! Fixed.
- Eliminate ASSERT when an attempt to free a USB device's address failed.
- In certain networking environments the AnywhereUSB would see ethernet Jumbo Frames and throw an exception. This has been fixed, although it is highly recommended that customers configure their switches to block transmission of Jumbo Frames to the Anywhere/USB if possible since it may affect the AnywhereUSB's performance.