WINC3400 Software

Release Notes

VERSION : **1.4.3**

DATE : **DEC-21**

Commented [CA-M1]: Under file-info-properties-advanced properties you will find some properties, the following will be automatically updated in the release process.

_ReleaseTR _ReleaseVerString _ReleasePlatform _ReleaseUmbrella _ReleaseRevision _ReleaseBranch

The release process copies the checked in document, updates the fileds and then renders it to a PDF file for the release package.

You should check in an updated version of the release note, filling in items like the last release in the custom properties, wherever things like the revision is required uset he properties (insert quick-parts…)

Abstract

This document presents an overview of the WINC3400 firmware release version 1.4.3, and corresponding driver.

1 Introduction

This document describes the WINC3400 version 1.4.3 firmware release package. This is a release containing Wi-Fi functionality with basic BLE support including an on-chip provisioning profile and custom BLE profiles using the Atmel BLE API and BluSDK.

The release package contains all the necessary components (binaries and tools) required to make use of the latest features including tools, and firmware binaries.

1.1 Highlights of the release

- Fixed:
  - "Fragattack" vulnerabilities:
    - CVE-2020-26140
    - CVE-2020-26143
    - CVE-2020-26144
    - CVE-2020-26146
    - CVE-2020-26147
    - CVE-2020-24588
  - Handling of QoS NULL frames in a Block Ack session
  - Removal of WEP support in firmware and driver
  - AP mode connection stability
  - Forwarding of ARP packets in AP mode
  - Smooth handling of multi stream TLS with 16KB record sizes
  - Enterprise security PMKSA caching
  - Improved TX gain table
  - TLS Rx memory leak

1.2 Firmware readiness

Microchip Technology Inc. considers version 1.4.3 firmware to be suitable for production release.

2 Release summary

2.1 Auditing information

Master Development Ticket : `https://jira.microchip.com/projects/W3400/versions/69048`

Wi-Fi:

Release Repository Branch :
http://svn.microchip.com/repo/wsg/Wifi_M2M/branches/rel_3400_1.4.3
Subversion Revision : **19455**

BLE:

Release Repository Branch : `/svn/Bluetooth/branches/ATWILC3400_BT_BLE_API`
Subversion Revision : **r7643**

BLE API:

Release Repository Branch : `/svn/Bluetooth/branches/ATWILC3400_BLE_API`
D21 Subversion Revision : **r7604**
SAM4 Subversion Revision : **r7604**

2.2 Version information

WINC Firmware version : 1.4.3
Host Driver version : 1.3.0
Host Interface Level : 1.5

RF version: 1.0

2.3 Released components

The release contains documentation, sources and binaries.

2.3.1 Documentation overview

The Application manuals, Release notes and Software API guides can be found in the `doc/` folder of the release package.

Release Notes:

This document

Software APIs:

WINC3400_IoT_SW_APIs.chm

WINC3400_BLE_APIs.chm

2.3.2 Binaries and programming scripts

The main 3400 firmware binary is in the `firmware` directory and named `m2m_aio_3400.bin`. This can be flashed to a WINC device using, for example, a serial bridge application available from ASF.

An OTA image is provided in the `ota_firmware` directory named `m2m_ota_3400.bin`.

2.3.3 Sources

Source code for the host driver can be found under the `src/host_drv` directory.

Source code for the tools, including crypto_lib) can be found under the `src/Tools` directory.

2.4 Release Comparison

Features in 1.4.2	Changes in 1.4.3
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN, WEP security. • WPA Personal Security (WPA1/WPA2), including protection against key re-installation attacks (KRACK). • WPA Enterprise Security (WPA1/WPA2) supporting: EAP-TTLSv0/MS-Chapv2.0 EAP-PEAPv0/MS-Chapv2.0 EAP-PEAPv1/MS-Chapv2.0 EAP-TLS EAP-PEAPv0/TLS EAP-PEAPv1/TLS • Simple Roaming Support	• Support for the WEP protocol is deprecated in 1.4.3. Attempts to configure it will result in error. • Countermeasures for 'Fragattack' vulnerabilities • Ensure PMKSA caching is attempted for WPA2 Enterprise connections.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN and WEP security modes. • The device cannot work as a station in this mode (STA/AP Concurrency is not supported).	• Support for the WEP protocol is deprecated in 1.4.3. Attempts to configure it will result in error. • Countermeasures for 'Fragattack' vulnerabilities • Fixed handling of source address when forwarding ARP packets out from the host.
WPS	
The WINC3400 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
TCP/IP Stack	
The WINC3400 has a TCP/IP Stack running in firmware side. It supports TCP and UDP full socket operations (client/server). The maximum number of supported sockets is currently configured to 12 divided as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server). • 1 RAW socket	No change
Transport Layer Security	
• The WINC3400 supports TLS v1.2, 1.1 and 1.0. • Client mode only. • Mutual authentication.	• Improved operation of multi-stream TLS RX with 16KB record size • Fix to TLS Alert handling • Fixed TLS RX memory leak when closing socket

• SHA384 and SHA512 support in X509 certificates processing. • Integration with ATECC508 (ECDSA and ECDHE support). • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128 _CBC_SHA256 (requires ATECC508) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)	
Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • SNTP	No change
Power saving Modes	

• The WINC3400 supports these powersave modes:
  ○ M2M_NO_PS
  ○ M2M_PS_DEEP_AUTOMATIC
• BLE powersave is always active
	No change

Device Over-The-Air (OTA) upgrade	
• The WINC3400 has built-in OTA upgrade. • Firmware is backwards compatible with driver 1.0.8 and later. • Driver is backwards compatible with firmware 1.2.0 and later (though the functionality will be limited by the firmware version in use).	No change
Wi-Fi credentials provisioning via built-in HTTP server	
The WINC3400 has built-in HTTP provisioning using AP mode (Open or WEP secured).	• WEP support has been removed
WLAN MAC only mode (TCP/IP Bypass, or Ethernet Mode)	
Allow WINC3400 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	No change

ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change
Miscellaneous features	
	Improved gain tables for module antenna
BLE functionality	
BLE 4.0 functional stack	No change

3 Test Information

This section summarizes the tests conducted for this release

3.1 Internal testing

Please refer to ticket Jira:W3400-689 for full details.

Testing was performed against the release candidate 1.4.3 against the following configuration(s):

H/W Version	:	WINC3400 XPRO module
Host MCU	:	ATSAMD21-XPRO

For Elliptic Curve cryptography support verification, a CRYPTOAUTH XPLAINED PRO board (containing an ECC508A chip) was inserted into the EXT2 socket on the ATSAMD21-XPRO board.

Testing was performed in both open air and shielded environments.

The following testing has been performed:

1. General functionality including:
    1. HTTP Provisioning
    2. BLE API verification
    3. Station Mode
    4. AP Mode
    5. IP (TCP and UDP client and server)
    6. HTTP POST/GET
    7. WPS (PIN and PushButton methods)
    8. Over-The-Air (OTA) update functionality and robustness (with and without TLS)

2. TLS functionality including:
    1. RSA ciphersuites:
        i. TLS_RSA_WITH_AES_128_CBC_SHA
        ii. TLS_RSA_WITH_AES_128_CBC_SHA256
        iii. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        iv. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        v. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

        Testing uses a 1024 bit server certificate, with a chain of 7 certificates of varying key lengths (1024,2048 and 4096 bit) leading to a 2048 bit root certificate.
    2. ECDSA ciphersuites:
        i. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

        Testing uses a NIST standard ECC P256 prime curve server certificate with two chains, one leading back to an ECC root certificate and the other leading to an RSA root certificate.
    3. SNI Client Hello extension
    4. Server certificate name validation
    5. Client authentication
    6. Amazon AWS IoT environment with client authentication and ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. MQTT connection, publishing and subscribing all succeed.
3. Performance under interference
4. Wi-Fi AP interoperability testing
5. Regression and longevity tests
6. TCP/IP stack robustness testing
    a. Using an internal implementation of IPerf.
    b. Verification of multi socket functionality

Known issues are declared in Section 4

4 Known Issues

Jira	Severity	Description
W3400-605	Medium	Prolonged heavy IP traffic load can result in the SPI becoming unusable between the WINC3400 and the host. Observed with SAMD21 host and WINC powersave disabled. Could potentially occur with other host platforms, but not yet observed. Recommended workaround: On SAMD21 host, the frequency of the issue can be minimized by using M2M_PS_DEEP_AUTOMATIC when transferring IP traffic. The issue could be detected by checking the return value of an API such as m2m_get_system_time(). A negative return value indicates that the SPI is unusable. If this occurs, reset the system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-621	Medium	The AP initiated group rekey process sometimes fails when the WINC is processing a high volume of receive traffic. Recommended workaround: Reconnect the Wi-Fi connection to the AP if a disconnection occurs due to this issue
W3400-102	Medium	During HTTP provisioning, if applications are running on the device being used to provision the WINC3400, they will not be able to access the internet during provisioning. Furthermore, if they attempt to do so, then the WINC3400 can become flooded with DNS requests and crash. This applies to HTTP provisioning only; BLE provisioning is unaffected. Also, this only applies if powersave is enabled. Recommended workarounds: (1) Use M2M_NO_PS when WINC3400 is in HTTP provisioning mode. (2) Close other internet applications (browsers, skype etc) before HTTP provisioning. If crash occurs, reset system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-40	Medium	The WINC3400 occasionally fails to proceed with 4-way handshake in STA mode, when using 11N WPA2. It does not send M2 after receiving M1. Recommended workaround: Retry the Wi-Fi connection.
W3400-293	Medium	1% of Enterprise conversations fail due to the WINC3400 not sending an EAP response. The response is prepared and ready to send but does not appear on the air. After 10 seconds the firmware times-out the connection attempt and the application is notified of the failure to connect.

		Recommended workaround: Configure the authentication server to retry EAP requests (with interval < 10 seconds). The application should retry the connection request when it is notified of the failure.
W3400-298	Medium	70% of Enterprise connection requests fail with a TP Link Archer D2 access point (TPLink-AC750-D2). The access point does not forward the initial EAP Identity Response to the authentication server. The issue is bypassed by PMKSA caching (WPA2 only), so reconnection attempts will succeed. Recommended workaround: The application should retry the connection request when it is notified of the failure.
W3400-461	Low	Sometimes the WINC3400 fails to see ARP responses sent from certain APs at 11Mbps. Recommended workaround: None. The ARP exchange will be retried several times and the response will eventually get through to the WINC3400.
W3400-60	Low	During BLE provisioning, the AP list is not cleaned up at the start of each scan request. As a result, the AP scan list can sometimes display duplicate or old scan entries. Recommended workaround: Only use one scan request during BLE provisioning.
W3400-59	Low	APIs at_ble_tx_power_get() and at_ble_max_PA_gain_get() return default values which do not correspond to the actual gain settings. Recommended workaround: None. Do not use these APIs.
W3400-30	Low	If the TLS server certificate chain contains RSA certificates with keys longer than 2048 bits, the WINC takes several seconds to process it. A Wi-Fi group rekey occurring during this time can cause the TLS handshake to fail. Recommended workaround: Retry opening the secure connection.
W3400-64	Low	at_ble_tx_power_set() needs special handling. Return values 0 and 1 should both be interpreted as successful operation. Refer to WINC3400_BLE_APIs.chm for more detail. Recommended workaround: Process the return value with care, according to the API documentation.
W3400-240	Low	After writing new firmware to the WINC3400, the first Wi-Fi connect attempt in STA mode takes an extra 5 seconds.

		Recommended workaround: Allow longer for the Wi-Fi connection to complete.
W3400-451	Low	When running in AP mode, the WINC3400 DHCP Server sometimes takes 5 to 10 seconds to assign an IP address. Recommended workaround: Allow longer for DHCP to complete.

5 New Features

There are no new features in this release.

6 Fixes and Enhancements

These are the fixes and enhancements since the previous released version (1.4.2).

6.1 Issues fixed

Jira ID	Description
W3400-688	**Sequence numbers from QoS NULL frames affect Block Ack operation** When a QoS NULL frame was received during a Block Ack session, the sequence number from the frame was incorrectly removed from the Block Ack scoreboard which could eventually result in the data transfer becoming stuck. Fixed: Ensure the Block Ack scoreboard is not updated on receipt of a QoS NULL frame.
W3400-683	**Some host MCUs lose SPI communication with the WINC3400 as it wakes up from sleep** When running the SPI bus at high speeds (around 40MHz), some hosts fail to read WINC registers over SPI around the WINC wakeup procedure. This results in loss of communication with the WINC. This has only been internally observed on a SAME54 host. Fixed: Decreasing the bus speed to around 10MHz during WINC wakeup fixes the problem. A framework has been added to the driver to allow the bus wrapper to lower the bus speed around WINC wakeup via calls to nm_bus_speed() which should be implemented on a per host basis. This function expects a single parameter – LOW or HIGH. When called with LOW, the bus speed should be decreased, and when called again with HIGH it should be reverted. On hosts that don't see this problem, nm_bus_speed() should just return M2M_SUCCESS.
W3400-677	**Occasional memory leak when closing a TLS socket** When closing a TLS socket, data that has been received by the WINC but not yet read by the host is sometimes not cleared up, leaking data buffers. Fixed: Ensure remaining data buffers are cleared up when the socket is closed.
W3400-672	**Plaintext data frames accepted in protected network (CVE-2020-26140, CVE-2020-26143, CVE-2020-26144)** Part of the 'Fragattack' vulnerabilities – plaintext QoS data frames received in a protected network were being processed and passed to the upper layers. Fixed: When in a protected network, drop plaintext non-EAPOL data frames
W3400-673	**Processes spoofed A-MSDU (CVE-2020-24588)** Receipt of a non-AMSDU frame that has been manipulated to look like an A-MSDU frame can establish an attack vector into the upper layers. Fixed: Check for a specifically crafted packet and discard if it is detected (fixed as per WFA security considerations 11/05/2021)

W3400-669	**Processes fragmented frame if 2nd fragment is plaintext (CVE-2020-26147)** In the case of CCMP, WINC would allow a plaintext fragment in a fragmented frame if the first fragment was CCMP encrypted. Fixed: Processing of fragmented frames is now performed in firmware, allowing a fix to be implemented.
W3400-670	**Processes fragmented frame if CCMP PN is not consecutive (CVE-2020-26146)** Fragments that have non-consecutive PN values were being accepted and processed. Fixed: Processing of fragmented frames is now performed in firmware, allowing a fix to be implemented.
W3400-668	**Incorrect return value from m2m_wifi_1x_get_option()** Driver function m2m_wifi_1x_get_option() returns the wrong status code in a particular code path. Fixed: Missing 'break' added.
W3400-666	**Received frames can get trapped in block ack reorder queue** When a non-AMPDU frame is received for a TID that has an active Block Ack session, the sender will not receive info on the WINCs Block Ack reorder queue, and previously missed frames may never be re-sent. Fixed: Drain the re-order queue whenever a non-AMPDU frame is received for a TID with an active Block Ack session.
W3400-660	**TLS ALERT messages received from the server are not always processed.** When the WINC3400 receives a TLS ALERT message after the TLS handshake has taken place, the message was not being processed correctly. Fixed: A bug in the alert handling code path was found and fixed.
W3400-654	**PMKSA caching not attempted for WPA2 Enterprise connections** WINC3400 is not using any cached PMKIDs in its connection attempts for WPA2 enterprise. Fixed: A bug in the enterprise connection code was found and fixed.

W3400-653	**Allow two TLS streams using large record sizes to operate concurrently.** Multiple TLS RX streams that were using record sizes of around 16K caused the WINC to run out of receive buffers, resulting in both streams becoming deadlocked. Fixed: TCP windowing has been reworked to allow for 2 TLS RX streams both using the maximum record size of 16K to operate concurrently.
W3400-631	**AP mode connection instability** In AP mode, an authentication attempt by a STA when there is already an ongoing authentication attempt can cause the WINC3400 to crash Fixed: The state machine has been adjusted to handle this scenario gracefully.
W3400-696	**Unknown OUI in message 3 of 4 way handshake causes failure** If an unknown OUI such as an AKM suite is contained in message 3 of the 4-way handshake, the handshake fails. Fixed: Ignore unknown OUIs in message 3 allowing the handshake to complete.

7 Appendix A – TLS Root certificates

The WINC3400 1.4.3 module comes with a preselected selection of TLS root certificates that will allow a TLS connection to be established with a range of internet TLS servers out of the box.

These preselected certificates are described in 7.1

7.1 TLS root certificates

Issuer	Filename	Expiry	Public Key	Signature Alg.	Notes
Amazon Root CA 1	AmazonRootCA1.cer	17 January 2038 01:00:00	RSA (2048 bits)	SHA256RSA	AWS Cloud
Baltimore CyberTrust Root	BaltimoreCyber-TrustRoot.cer	13 May 2025 00:59:00	RSA (2048 bits)	SHA1RSA	Azure Cloud
DigiCert High Assurance EV Root CA	DigiCert.cer	10 November 2031 01:00:00	RSA (2048 bits)	SHA1RSA	
DigiCert High Assurance EV Root CA	DigiCertSHA2.cer	22 October 2028 13:00:00	RSA (2048 bits)	SHA256RSA	
Entrust Root Certification Authority	EnTrust.cer	27 November 2026 21:53:42	RSA (2048 bits)	SHA1RSA	
GlobalSign Root CA	GlobalSignRoot.cer	28 January 2028 13:00:00	RSA (2048 bits)	SHA1RSA	
Internet Security Research Group Root X1	isrgrootx1.cer	04 June 2035 12:04:38	RSA (4096 bits)	SHA256RSA	LetsEncrypt
QuoVadis Root CA 2	QuoVadis_Root.cer	24 November 2031 19:23:33	RSA (4096 bits)	SHA1RSA	
VeriSign Class 3 Primary Certification Authority	VeriSign.cer	17 July 2036 00:59:59	RSA (2048 bits)	SHA1RSA	

8 Terms and Definitions

Term	Definition
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CBC	Cyclic Block Chaining
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name Server
DTIM	Directed Traffic Indication Map
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESS	Extended Service Set (infrastructure network)
GAP	Generic Access Profile
HTTP	Hypertext Transfer Protocol
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NDIS	Network Driver Interface Specification
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PMK	Pair-wise Master Key
PSK	Pre-shared Key
RSA	Rivest-Shamir-Adleman (public key cryptosystem)
RSN	Robust Security Network
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Strength Signal Indicator
TIM	Traffic Indication Map
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WINC	Wireless Network Controller
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)