

Zyxel WAH7706 Release Note

CONFIDENTIAL

Date:	2018 / 06 / 15
SW Version:	V1.00(ABBC.9)C0
Doc Version :	V1.0

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.9)C0
- **FW change notes:**
 - Features:
 - Apply new battery level definition
 - Add Vodafone Iceland and TDC Norway to the auto APN list
 - Change DHCP max lease time to 14400 minutes
 - Fixed Bugs:
 - curl: CVE-2016-8615, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8623, CVE-2016-8617, CVE-2016-8624, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101
 - zlib: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843,
 - glibc: CVE-2015-5180, CVE-2017-1000366, CVE-2017-8804, CVE-2017-15670
 - wpa-suplicant: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088
 - Limitations:
 - WAH7706 V1.00(ABBC.3)C0 or previous version firmwares can't block old LTE4506's firmwares from loading to the WAH7706.
 - The new firmware upgrade protection mechanism is not applied to TR-069 firmware upgrade function
 - Known issues:
 - Small Screen provide "PLMN Mode: Auto/Manual and PLMN Scan/Selection" function, but after setting that will make the mismatch between the Desktop version
 - Manual PLMN(Auto RAT) selection is malfunction if before force PLMN+2G/3G/4G(Specific RAT)

If user forced specific RAT PLMN selection then PLMN selection with Auto RAT malfunction.
The previous forced PLMN+RAT (e.g. 2G) will keep using until change back to auto PLMN selection.

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.8)C0
- **FW change notes:**
 - Features:
 - Web UI password fields must be masked.
 - Charging cutoff voltage is 4.2V and temperature is 55 degree Celsius.
 - Wi-Fi setting update (RED certification)
 - Adjust EDCCA threshold
 - disable roaming function
 - Support GT SIM card (GT is one of the Taiwanese LTE service providers).
 - Fixed Bugs:
 - Fix command injection in Web UI NTP page
 - Fix the issue "device can't boot while user cut off device power in boot stage (RMA case)".
 - Upgrade OpenEmbedded to morty-16.0.2
 - openssl: Security fix CVE-2016-7055
 - openssl: CVE: CVE-2017-3731
 - libxml2: Security fix CVE-2016-5131
 - libxml2: fix CVE-2016-4658
 - libxml2: CVE-2016-9318
 - busybox: Security fix CVE-2016-6301
 - bash: fix CVE-2016-9401
 - bash: CVE-2016-0634
 - glibc: Security fix CVE-2016-6323
 - Upgrade dnsmasq to version 2.76
 - Fix CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496
 - Fix busybox CVE-2017-15873/15874
 - Update TR-069 to the latest version
 - Keep Password, Username, Connection Request Password, Connection Request Username after SPV.

- Upgrade gSOAP version to 2.7.17
 - Upgrade gSOAP HTTP-DA plugin to 2.8.31
 - Fix memory leaks
 - Set soap timeout to 10 seconds
 - Fix Samba CVE-2017-15275
 - Fix iOS App TIOD can't access samba
 - TR-069: include the latest fixes, set PeriodicInformInterval as 86400 seconds
 - Fix Linux CVE-2017-2636
 - Samba CVE-2017-7494
- Limitations:
- WAH7706 V1.00(ABBC.3)C0 or previous version firmwares can't block old LTE4506's firmwares from loading to the WAH7706.
 - The new firmware upgrade protection mechanism is not applied to TR-069 firmware upgrade function
- Known issues:
- Small Screen provide "PLMN Mode: Auto/Manual and PLMN Scan/Selection" function, but after setting that will make the mismatch between the Desktop version
 - Manual PLMN(Auto RAT) selection is malfunction if before force PLMN+2G/3G/4G(Specific RAT)
 - If user forced specific RAT PLMN selection then PLMN selection with Auto RAT malfunction.
 - The previous forced PLMN+RAT (e.g. 2G) will keep using until change back to auto plmn slection.

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.7)C0
- **Modem ver.:** MPSS.BO.2.5.1.c1-00106-M9635TAAANAZM-1
- **FW change notes:**
 - New Features:
 - Implement new web GUI login policy: a stricter “change password” rules.
 - Implement new web GUI login policy: block 5 minutes after 3 failed login attempts
 - PLMN selection
 - Add DMZ
 - New Protection mechanism when upgrading firmware - from this version, device cannot upgrade old version and firmware not for this sku.
 - Fixed Issues:
 - TR-069 not start issue
 - Read only, not allow for writing with Design feedback, “Device.Cellular.AccessPoint.{i}.Enable”, then the Fault code 9001: Request denied (no reason specified) should be indicated at the Response to Server not accept SPV but no action.
 - Registered TR069 Setting has to indicate the success Registered setting. But display the last trial if no registered server.
 - The TR-069 parameter “Device.Cellular.Interface.{i}.Stats.X_“A0XXXX”_SupportedBand” has to support R/W but it is dependent on Supported bands of the device.
 - On the LTE4506, the response of the TR-069 parameter “Device.Cellular.Interface.{i}.Enable” should be Fault code 9001: Request denied (no reason specified) because the interface is the only interface which also bears the TR-069 connection. The LTE4506 can accept SPV but without any action.
 - The web GUI does not support to change PDN Type but there is a TR-069 parameter supporting this function.

- CWMP Certificate Validation Vulnerability [Not validate the ACS certificate (CWE-295)]
- The device fails to establish the SSL TR069 connection with Zyxel ACS
- Missing Functions for TR069 CA file management at Generic FW. Function: CA file import and CA file information [Import Certificate file & Current TR-069 Certificate file]
- The connection request port setting is not the standard port, i.e. port 51005; instead it is port 7547.
- There is no TRANSFER COMPLETE event report to ACS that causes firmware upgrade failure from ACS' perspective.
- Limitations:
 - WAH7706 V1.00(ABBC.3)C0 or previous version firmwares can't block old LTE4506's firmwares from loading to the WAH7706.
 - The new firmware upgrade protection mechanism is not applied to TR-069 firmware upgrade function
- Known issues:
 - Small Screen provide "PLMN Mode: Auto/Manual and PLMN Scan/Selection" function, but after setting that will make the mismatch between the Desktop version
 - Manual PLMN(Auto RAT) selection is malfunction if before force PLMN+2G/3G/4G(Specific RAT)
 - If user forced specific RAT PLMN selection then PLMN selection with Auto RAT malfunction.
 - The previous forced PLMN+RAT (e.g. 2G) will keep using until change back to auto plmn slection.

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.6)C0, (WAH7706_m00.00_v01.08.1607120)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - New Features:
 - PLMN selection
 - Block user login for 5 minutes after 3 failed login attempt
 - New APN list
 - Fixed Issues:
 - TR-069 not started issue
 - Add back "internet.saunalahti" APN in the auto APN list
 - English grammar issues:
 - ◆ 1. Login to the device GUI, scroll to the Wi-Fi tab> Wi-Fi Status; message is displayed as "SSID is not enable", this should be fixed to read "SSID is not enabled"
 - ◆ 2. Load a firmware file and upgrade firmware. The message is displayed as "Upgrade will begin, please don't refresh the browser, otherwise the upgrading may be failed.", this should be fixed to read "Firmware upgrade will begin, please don't refresh the browser or switch off your device; otherwise the Firmware upgrade may fail."
 - IPv6 issue

Information

- **HW ver.:** EPR
- **FW ver.:** **V1.00(ABBC.5)C0**, (WAH7706_m00.00_v01.08.1607120)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - Fixed WIFI IOT Issues
 - Details
 - Change WIFI encryption mode to WPA2 only
 - Add first release of QCA patches to fix iPhone connection issue when switching 2.4G/5G.
 - Add second release of QCA patches
 - Add internal WIFI patches

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.4)C0, (WAH7706_m00.00_v01.08.1605070)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - Update new samba tool
 - Add DST feature
 - Add connecting/disconnecting status on the home page
 - Fix TR-069 issue:
 - Issue#14 TR069 Remote FW upgrade failure, if HFS provides HTTPS URL of the FW then the download process will not finish and also no response code to inform ACS
 - Issue#15 TR069 Remote FW upgrade failure, if HFS provides the file with username/password protect. Then process will block and all connection between ACS. Device need to reboot
 - Issue#16:""0 BOOTSTRAP"" not sent after ACS URL has been modified in any way
 - Issue#18 Through ACS to change the ""Device.ManagementServer.URL"" but keep alive with original ManagementServer.URL
 - Fix issue 6: The static USB_net0 Host is not displayed on Connected devices page
 - Fix TR-069 IOT issue:
 - Modify soap "User-Agent" from "gSOAP/2.7" to "Zyxel-gSOAP/2.7"
 - Specify the xsd type in parameter value structure
 - Fixed can't upgrade FW if specify the file size as 0
 - Fixed 401 UNAUTHORIZED issue
 - Fixed FW upgrade fail if filename contains white space characters
 - issue bootstrap event after change the ACS URL
 - issue the transfer complete event and MDownload event after FW upgrade reboot
 - Disable periodic inform while downloading

- support SSL
- support download file from https URL
- Fix most bugs found on LTE4506
 - Fix LTE4506 issue 11: Without wrong upgrade bin file protect mechanism that will cause device crash
- Base on (ABBC.3)C0 version and add one patch to fix one SMS issue which report from customer

Information

- **HW ver.:** EPR
- **FW ver.:** **V1.00(ABBC.3)C0**, (WAH7706_m00.00_v01.08.1602250)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - eglibc: fix CVE-2015-7547

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.2)C0, (WAH7706_m00.00_v01.08.1601200)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - DUT can connect to internet after set incorrect apn when network is 4G mode.
 - Add multi-language
 - Add max Wi-Fi client setting
 - When current statistics of received count to 4GB and it will reset to count from 0 .
 - The WPS GUI will display abnormal
 - WWAN Power Saving doesn't work.

Information

- **HW ver.:** EPR
- **FW ver.:** V1.00(ABBC.1)C0 (WAH7706_m03.04_v01.08.1511100)
- **Modem ver.:** MPSS.BO.2.0.1.c3.12-00010-M9635TAAAANAZM-1
- **FW change notes:**
 - Only check enable URL Filter,can't surf the internet.
 - The function of URL Filter fails.
 - The web ui will often pop up the prompt: It is not in login state.Reenter please!
 - There is no data usage limit prompt in LCM when check "Enable Data Limit" again
 - The attempts remaining times displays wrongly when input incorrect PIN code
 - LTE Band 20 /28/38 execute handover or redirection to WCDMA Band1/8 are fail
 - The GUI will crash when insert a sd card with exFAT format.
 - Auto APN setting is not correct.
 - Manual APN settings not work with User Name and password.
 - WiFi design problem