

# **EX7501-B0\_Generic**

Firmware Release Note

V5.18(ACHN.2.1)C0

Date: April 18 2025  
Author: Yuan Lin  
Reviewer: Ryan Yeh

**THIS DOCUMENT CONTAINS PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THE Zyxel AND SHOULD NOT BE DISCLOSED TO OTHERS IN WHOLE OR IN PART, REPRODUCED, COPIED, OR USED AS BASIS FOR DESIGN, MANUFACTURING OR SALE OF APPARATUS WITHOUT WRITTEN PERMISSION OF Zyxel.**

## TABLE OF CONTENTS

REVISION HISTORY.....	3
SUPPORTED PLATFORMS:.....	4
VERSIONS: .....	4
NOTES:.....	4
PUBLIC DOMAIN SOFTWARE ANNOUNCEMENTS .....	5
KNOWN ISSUES.....	8
MODIFICATIONS IN V5.18(ACHN.2.1)C0.....	8
MODIFICATIONS IN V5.18(ACHN.2.1)B1 .....	8
MODIFICATIONS IN V5.18(ACHN.2)C0 .....	8
MODIFICATIONS IN V5.18(ACHN.2)B3.....	9
MODIFICATIONS IN V5.18(ACHN.2)B2.....	10
MODIFICATIONS IN V5.18(ACHN.1)C0 .....	11
MODIFICATIONS IN V5.18(ACHN.1)B4.....	11
MODIFICATIONS IN V5.18(ACHN.1)B3.....	12
MODIFICATIONS IN V5.18(ACHN.1)B2.....	13
MODIFICATIONS IN V5.18(ACHN.1)B1.....	14
MODIFICATIONS IN V5.18(ACHN.0)C0 .....	16
MODIFICATIONS IN V5.18(ACHN.0)B6.....	16
MODIFICATIONS IN V5.18(ACHN.0)B5.....	16
MODIFICATIONS IN V5.18(ACHN.0)B4.....	16
MODIFICATIONS IN V5.18(ACHN.0)B3.....	17
MODIFICATIONS IN V5.18(ACHN.0)B2.....	18
MODIFICATIONS IN V5.18(ACHN.0)B1.....	22

## Revision History

Date	Release	Author	Description
2023/02/24	1.0	Yuan Lin	FW release for V5.18(ACHN.0)b1
2023/04/28	1.1	Yuan Lin	FW release for V5.18(ACHN.0)b2
2023/06/16	1.2	Yuan Lin	FW release for V5.18(ACHN.0)b3
2023/07/28	1.3	Yuan Lin	FW release for V5.18(ACHN.0)b4
2023/08/11	1.4	Yuan Lin	FW release for V5.18(ACHN.0)b5
2023/09/01	1.5	Yuan Lin	FW release for V5.18(ACHN.0)b6
2023/09/22	1.6	Yuan Lin	FW release for V5.18(ACHN.0)C0
2023/10/19	2.1	Yuan Lin	FW release for V5.18(ACHN.1)b1
2023/12/15	2.2	Yuan Lin	FW release for V5.18(ACHN.1)b2
2024/03/01	2.3	Yuan Lin	FW release for V5.18(ACHN.1)b3
2024/03/29	2.4	Yuan Lin	FW release for V5.18(ACHN.1)b4
2024/04/24	2.5	Yuan Lin	FW release for V5.18(ACHN.1)C0
2024/10/18	3.1	Yuan Lin	FW release for V5.18(ACHN.2)b2
2025/01/03	3.2	Yuan Lin	FW release for V5.18(ACHN.2)b3
2025/02/21	3.3	Yuan Lin	FW release for V5.18(ACHN.2)C0
2025/04/11	4.1	Yuan Lin	FW release for V5.18(ACHN.2.1)b1
2025/04/18	4.2	Yuan Lin	FW release for V5.18(ACHN.2.1)C0

## **EX7501-B0\_Generic V5.18(ACHN.2.1)C0 Release Note**

Date: April 18 2025

### **Supported Platforms:**

Zyxel EX7501-B0

### **Versions:**

Bootbase version : V2.4 | 12/15/2023 16:09:13

Firmware version : V5.18(ACHN.2.1)C0

Kernel version: 4.19.183

WLAN code version: 17.10.188.75

3G WWAN package version: 1.26

### **Notes:**

Linux console:

# uname -a

# wl ver

# wwanpackage info

## Public Domain Software Announcements

Open Source Used In Product	Version	From (Source)	License Terms	Modified / Used
attr	2.5.1	<a href="http://savannah.nongnu.org/projects/attr">http://savannah.nongnu.org/projects/attr</a>	GPL-2.0-only	Used
atftp	0.8.0	<a href="https://sourceforge.net/projects/atftp/">https://sourceforge.net/projects/atftp/</a>	GPL-2.0-only	Modified
Bridge-Utils	1.7.1	<a href="http://bridge.sourceforge.net">http://bridge.sourceforge.net</a>	GPL-2.0-only	Used
BusyBox	1.31.1	<a href="http://www.busybox.net/">http://www.busybox.net/</a>	GPL-2.0-only	Modified
clinkc	2.4	<a href="http://sourceforge.net/projects/clinkc/">http://sourceforge.net/projects/clinkc/</a>	BSD-3-Clause	Modified
conntrack- tools	1.4.5	<a href="https://git.netfilter.org/conntrack-tools/">https://git.netfilter.org/conntrack-tools/</a>	GPL-2.0-only	Used
dnsmasq	2.85	<a href="http://www.thekelleys.org.uk/dnsmasq/doc.html">http://www.thekelleys.org.uk/dnsmasq/doc.html</a>	GPL-2.0-only	Modified
dropbear	2024.85	<a href="http://matt.ucc.asn.au/dropbear/dropbear.html">http://matt.ucc.asn.au/dropbear/dropbear.html</a>	MIT	Modified
ebtables	2.0.10-4	<a href="http://ebtables.sourceforge.net">http://ebtables.sourceforge.net</a>	GPL-2.0-only	Modified
eventlog	0.2.10	<a href="http://git.balabit.hu/?p=bazsi/eventlog-1.0.git;a=summary">http://git.balabit.hu/?p=bazsi/eventlog-1.0.git;a=summary</a>	BSD-3-Clause	Used
expat	2.6.2	<a href="http://expat.sourceforge.net/">http://expat.sourceforge.net/</a>	MIT	Used
ez-ipupdate	3.0.11b8	<a href="http://ez-ipupdate.com/">http://ez-ipupdate.com/</a>	GPL-2.0-only	Used
gettext	0.19.8.1	<a href="http://www.gnu.org/software/gettext/">http://www.gnu.org/software/gettext/</a>	GPL-2.0-only	Used
Glib	2.68.1	<a href="http://www.gtk.org/">http://www.gtk.org/</a>	LGPL-2.0-only	Used
iproute2	2.5.7.0	<a href="http://repository.timesys.com/buildsources/i/iproute2/">http://repository.timesys.com/buildsources/i/iproute2/</a>	GPL-2.0-only	Modified
iptables	1.8.5	<a href="http://www.netfilter.org">http://www.netfilter.org</a>	GPL-2.0-only	Modified
json-c	0.13.1	<a href="https://github.com/json-c/json-c/downloads">https://github.com/json-c/json-c/downloads</a>	MIT	Modified
libedit	20080712-2.11	<a href="http://pkgs.fedoraproject.org/repo/pkgs/libedit/libedit-20080712-2.11.tar.gz/">http://pkgs.fedoraproject.org/repo/pkgs/libedit/libedit-20080712-2.11.tar.gz/</a>	BSD-3-Clause	Modified
libffi	3.3	<a href="http://pkgs.fedoraproject.org/repo/pkgs/libffi/libffi-3.0.11.tar.gz/">http://pkgs.fedoraproject.org/repo/pkgs/libffi/libffi-3.0.11.tar.gz/</a>	MIT	Used
libiconv	1.11.1	<a href="http://www.gnu.org/software/libiconv/">http://www.gnu.org/software/libiconv/</a>	LGPL-2.0-only	Modified
libnetfilter_co nntrack	1.0.7	<a href="https://git.netfilter.org/libnetfilter_conntrack/">https://git.netfilter.org/libnetfilter_conntrack/</a>	GPL-2.0-only	Used
libnetfilter_qu eue	1.0.3	<a href="http://www.netfilter.org/projects/libnetfilter_queue/">http://www.netfilter.org/projects/libnetfilter_queue/</a>	GPL-2.0-only	Used

libnftnl	1.0.1	<a href="http://www.netfilter.org/projects/libnetfilter_queue/">http://www.netfilter.org/projects/libnetfilter_queue/</a>	GPL-2.0-only	Used
libpcap	1.9.1	<a href="http://www.tcpdump.org">www.tcpdump.org</a>	BSD-3-Clause	Used
libtool	2.4.6	<a href="http://www.gnu.org/software/libtool/">http://www.gnu.org/software/libtool/</a>	GPL-2.0-only	Used
libusb	1.0.9	<a href="http://www.libusb.org/">http://www.libusb.org/</a>	LGPL-2.1-only	Used
libxml2	2.9.12	<a href="http://xmlsoft.org/sources/">http://xmlsoft.org/sources/</a>	MIT	Used
logrotate	3.22.1	<a href="https://launchpad.net/ubuntu/hardy/i386/logrotate/">https://launchpad.net/ubuntu/hardy/i386/logrotate/</a>	GPL-2.0-only	Modified
mailsend	1.17b15	<a href="https://github.com/muquit/mailsend/">https://github.com/muquit/mailsend/</a>	BSD-3-Clause	Modified
ncurses	6.1	<a href="http://ftp.gnu.org/pub/gnu/ncurses/">http://ftp.gnu.org/pub/gnu/ncurses/</a>	MIT	Modified
net-snmp	5.9.4	<a href="http://www.net-snmp.org/">http://www.net-snmp.org/</a>	BSD-3-Clause	Modified
ntfs-3g	2022.10.3	<a href="http://ntfs-3g.org">http://ntfs-3g.org</a>	GPL-2.0-only	Used
ntpclient	2007_365	<a href="http://doolittle.icarus.com/ntpclient/">http://doolittle.icarus.com/ntpclient/</a>	GPL-2.0-only	Modified
nghttp2	1.57.0	<a href="https://osdn.net/projects/immortalwrt/storage/sources/nghttp2-1.43.0.tar.xz/">https://osdn.net/projects/immortalwrt/storage/sources/nghttp2-1.43.0.tar.xz/</a>	MIT	Used
openssl	3.2.0	<a href="http://www.openssl.org">http://www.openssl.org</a>	OpenSSL	Modified
Popt	1.16	<a href="http://rpm5.org/files/popt/">http://rpm5.org/files/popt/</a>	MIT	Modified
ppp	2.4.3	<a href="http://www.roaringpenguin.com/pppoe">http://www.roaringpenguin.com/pppoe</a>	GPL-2.0-only	Modified
pure-ftpd	1.0.50	<a href="http://pureftpd.org">http://pureftpd.org</a>	ISC	Modified
radvd	1.8	<a href="http://www.litech.org/radvd/">http://www.litech.org/radvd/</a>	BSD-3-Clause	Used
readline	8.2	<a href="http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html">http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html</a>	GPL-2.0-only	Used
samba	3.6.25	<a href="http://www.samba.org/samba/">http://www.samba.org/samba/</a>	GPL-2.0-only	Modified
Sqlite	3.46.0	<a href="http://www.sqlite.org/">http://www.sqlite.org/</a>	Public-Domain	Used
syslog-ng	4.7.1	<a href="http://www.balabit.com/network-security/syslog-ng/">http://www.balabit.com/network-security/syslog-ng/</a>	GPL-2.0-only	Used
tcpdump	4.99.4	<a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a>	BSD-3-Clause	Used
udhcp	0.9.8	<a href="http://udhcp.busybox.net/">http://udhcp.busybox.net/</a>	GPL-2.0-only	Modified
usb-modeswitch	2.1.0	<a href="http://www.draisberghof.de/usb_modeswitch/">http://www.draisberghof.de/usb_modeswitch/</a>	GPL-2.0-only	Used
WIDE-DHCPv6	20080615	<a href="http://wide-dhcpv6.sourceforge.net/">http://wide-dhcpv6.sourceforge.net/</a>	BSD-3-Clause	Modified
miniupnpd	2.3.1	<a href="https://github.com/miniupnp/miniupnp">https://github.com/miniupnp/miniupnp</a>	BSD-3-Clause	Used
curl	8.7.1	<a href="https://curl.se/">https://curl.se/</a>	MIT	Modified
quagga	1.2.4	<a href="https://github.com/Quagga/quagga">https://github.com/Quagga/quagga</a>	GPL-2.0-only	Used



## Known issues

Modules	Issue	Risk Impact Information

### [NOTE]

#### 1. OpenSSL 3.1.2 Upgrade Notification

The certificates signed using SHA1 or older/weaker hashes are no longer supported for authenticating servers or clients.

Before upgrading the firmware:

- Please ensure that certificates in your devices are not using weak hashes.
- If weak hashes are detected, kindly update and verify your certificates promptly with stronger hash  
(The minimum recommended hash is SHA256)

## Modifications in V5.18(ACHN.2.1)C0

### ● Feature Enhancement

Modified Modules	Features Enhancement List
FCS	Based on V5.18(ACHN.2.1)b1, Change to FCS version

## Modifications in V5.18(ACHN.2.1)b1

Based on V5.18(ACHN.2)C0 to release V5.18(ACHN.2.1)b1

### ● Feature Enhancement

Modified Modules	Features Enhancement List
Security	EN18031 OPAL20 product compliance release
GUI	WEB GUI meets the request of Europe EAA (European Accessibility Act)

### ● Bug Fixed

## Modifications in V5.18(ACHN.2)C0

Based on V5.18(ACHN.2)b3 to release V5.18(ACHN.2)C0



## Modifications in V5.18(ACHN.2)b3

Based on V5.18(ACHN.2)b2 to release V5.18(ACHN.2)b3

### ● Feature Enhancement

Modified Modules	Features Enhancement List
Log	[EN18031][Log] Add some logs when end users change their profile on GUI
SSH	[EN18031][SSH] Remove insecure cipher suit for dropbear SSH
CVE	[EN18031][CVE] Fixed CVE libxml2 : CVE-2022-23308, CVE-2022-40303, CVE-2024-25062 nghttp2 : CVE-2023-35945, CVE-2023-44487 pppd : CVE-2006-2194, CVE-2014-3158, CVE-2015-3310, CVE-2018-11574, CVE-2020-8597

### ● Bug Fixed

Modified Modules	Bug Fixed List
GUI	[GUI] When the wireless clients connect to CPE's WiFi, but GUI does not show "Band" in Connectivity page
TR-181	[TR-181] GPV ['Device.WiFi.NeighboringWiFiDiagnostic.DiagnosticsState'] but it display None.
TR-143	[TR-143] SPV {'Device.IP.Diagnostics.UploadDiagnostics.TestFileLength': '10485760'} but CPE return 9003 fault code
TR-369	[TR-369] Can't set multiple parameter via TR-369 at same time. [TR-369] CPE cannot upgrade FW via TR-369. [TR-369] Can't modify CPE LAN IP and Subnet Mask via TR-369. [TR-369] SPV wifi config via TR-369 at same time, SSID and password will not changed.
MPro Mesh	[MPro Mesh][ZyXel One_Agent] After Onboarding RP_Agent success, it cause RP_agent "wapp" daemon disappear. [MPro Mesh][ZyXel One_Agent] Enable guest wifi via APP, it will lead two RP_Agent auto config fail.

	[MPro Mesh][Zyxel One_Agent] Enable guest wifi via APP, it will lead two RP_Agent auto config fail.
Vulnerability	[CVE-2024-12009] Zyxel-SI-1591 [Vulnerability] Post-authentication command injection vulnerability in the function "ZyEE" [CVE-2024-12010] Zyxel-SI-1592 [Vulnerability] Post-authentication command injection vulnerability in the email sending function

## Modifications in V5.18(ACHN.2)b2

Based on V5.18(ACHN.1)C0 to release V5.18(ACHN.2)b2

### ● Feature Enhancement

Modified Modules	Features Enhancement List
TR-369	[eITS#230900654][AXIROS] implementation request / WebSocket [eITS#231000272][AXIROS] Certificate management for websocket [eITS#231001817] Web GUI configuration for websocket
Security	[Security][TSA] V.E.4 : Downgrade protection. [Enhance] Open Source Packages Upgrade - Phase
APP	[APP] Zyxel One APP implement
System	[eITS#240301447] Guest WiFi password scheme enhancement [eITS#240801627] Conditional ROM convert for Guest WiFi password scheme enhancement [eITS#240200611]EX5601, MAP-T issue with s46-portparams [eITS#240600337] DHCP option 43 - ACS information [eITS#240701741]Add "gateway IP and connection up time for WAN and WLAN client" in system Info page.
GUI	[GUI] Will not force Web http redirect to https.

### ● Bug Fixed

Modified Modules	Bug Fixed List
------------------	----------------

Mesh	[MPro Mesh_Agent] When turn off APP LED in Home page icon, Controller LED will dark but all AP/RP_Agent still on.
System	[System] The Wired Client's LinkSpeed should display 1000M/Full instead of 1000/Full.
Vulnerability	[CVE-2024-5412][Zyxel-SI-1557][Vulnerability] Unauthenticated heap buffer overflow in the libclinkc library [CVE-2024-38266,38267,38268,38269][Zyxel-SI-1559][Vulnerability] Multiple authenticated buffer overflow vulnerabilities in VMG8825-T50 [CVE-2024-8748][Zyxel-SI-1576][Vulnerability] Unauthenticated buffer overflow in VMG8825-T50 [CVE-2024-9197][Zyxel-SI-1583][Vulnerability] Buffer overflow and potential command injection vulnerabilities in VMG3625-T50B (Medium)
Security	[Security] SSH Weak Host Key Algorithm [Security] SNMP Agent Default Community Name (public, private)

## Modifications in V5.18(ACHN.1)C0

Based on V5.18(ACHN.1)b4 to release V5.18(ACHN.1)C0

- **Feature Enhancement**
- **Bug Fixed**

## Modifications in V5.18(ACHN.1)b4

Based on V5.18(ACHN.1)b3 to release V5.18(ACHN.1)b4

- **Feature Enhancement**
- **Bug Fixed**

Modified Modules	Bug Fixed List
TR-369	[TR-369] When set Controller Alias with space, GUI will add cpe- automatically. [DST] TR-369 setting does not match DST
Parental Control	[eITS#240301182] EX7501, Conditionally unable to open Connectivity List and add new Parental Control rule

TR-069	[eITS#240200784] GPN Device.WiFi. fail [eITS#240101401] CPE cannot receive Some Incoming Calls after Huawei adds the new SIP service port 5062 to the Soft Switch (SS).
--------	--

## Modifications in V5.18(ACHN.1)b3

Based on V5.18(ACHN.1)b2 to release V5.18(ACHN.1)b3

### ● Feature Enhancement

Modified Modules	Features Enhancement List
System	[eITS#230400862] LED control [eITS#231200465] OPAL family, Feature improvement request - WAN ip lease time

### ● Bug Fixed

Modified Modules	Bug Fixed List
TR-143	[TR-143] HTTP Download Diagnostic cannot pass PQA criteria. [TR-143] HTTP Upload Diagnostic cannot pass PQA criteria. [Performance] Iperf Upload throughput can't pass PQA criteria (criterion is 9G)
System	[System] MQTT client password is not encrypted in backup config file.
WAN	[WAN] CPE cannot create ip tunnel when enable DS-Lite with Manually Configured and IP format [WAN] Delete default wan interface can't open traffic status page.
UPnP	[UPnP] Click UPnP icon will not redirect to GUI.
NAT	[NAT] After change DUT http MGMT port, UPnP info on PC Network Infrastructure not change
QoS	[QoS] Shaper Profile for WAN Interface cannot work if the WAN change IP address
WLAN	[WLAN] When WiFi password is 64 characters (without uppercase letter, lowercase letter and special character), GUI still can save it.

Vulnerability	[Vulnerability] Zyxel-SI-1536 [Vulnerability] Buffer overflow vulnerability in the "traceroute" command
GUI	[GUI] Traffic Status>LAN page has an extra column of 0. [GUI] When MESH is enabled. the wifi client's information in Connectivity \ List page can include RSSI information

## Modifications in V5.18(ACHN.1)b2

Based on V5.18(ACHN.1)b1 to release V5.18(ACHN.1)b2

### ● Feature Enhancement

Modified Modules	Features Enhancement List
System	[eITS#231000756]Feature Request - DHCP opt 12 [eITS#231101419] How to change DOS Protection Blocking with TR098 [eITS#231000006]ZYX-593 IoT SSID (FRQ to propagate 3 parameters from the controller to the agents)

### ● Bug Fixed

Modified Modules	Bug Fixed List
MGMT	[MGMT] GUI cannot be accessed after https port is changed to 80.
System	[System] The Backup config file cannot save settings of TR-369 Local Agent [System] Partial Factory Reset via TR-181 cannot reset CPE successfully [System] Login to "User" account should not have permission to modify WiFi and LAN settings on Card page [System] Create 3~4 EEs and enable all, then GUI will keep loading in "ZyEE Monitor" page
VoIP	[VoIP] SIP account register fail when WAN set multi-wan and SIP provider bonding multi-wan. [VoIP] In VoIP SIP Provider 2, RTP Port Range is 40000~40018
WAN	[WAN] WWAN can NOT dial successfully [WAN] The CPE LAN cannot get IPv6 address if PPPoE WAN is

	<p>IPv6 only and DS-Lite enabled by automatically configured by DHCP.</p> <p>[WAN] Traffic Status page cannot display complete WAN entry</p> <p>[WAN] MAP-E and MAP-T cannot surf to Internet by IPv4.</p>
MPro Mesh	<p>[MPro Mesh] When the signal is strong, the expander should not form a daisy chain topology.</p> <p>[MPro Mesh_Agent] When Android clients press "WiFi" option via APP, it will lead APP crash.</p> <p>[MPro Mesh_Agent] When disable controller's MESH, APP should not to login.</p> <p>[MPro Mesh] Disable Controller Mesh then Enable via TR or GUI, GUI already display enable correctly but it didn't enable mesh successfully.</p>
TR-069	<p>[TR-069] CPE cannot upload configuration via TR-069 when FileType is "3 Vendor Configuration File".</p> <p>[TR-181] Add new PPPoE WAN via ACS, but it cannot get IP and display on System Info page.</p> <p>[TR-181] ACS SPV to do Neighboring WiFi Diagnostics , but the results only contains 5GHz information.</p> <p>[TR-181] ACS GPV "Device.XMPP.Connection.{i}.Password", and it should be an empty string.</p>
MLD	[MLD] LAN Client cannot play MLD until disable DDOS
WLAN	<p>[WLAN] The Wi-Fi others Bands value should not include 6GHz</p> <p>[WLAN] When Wi-Fi 2.4G is disable, press 2.4G Scan wireless LAN Channels. GUI pop out incorrect warning message.</p>
GUI	[GUI] XMPP Password should not be plaintext on GUI.

## Modifications in V5.18(ACHN.1)b1

Based on V5.18(ACHN.0)C0 to release V5.18(ACHN.1)b1

### ● Feature Enhancement

Modified Modules	Features Enhancement List
System	<p>[eITS#220400813] Container based F-secure</p> <p>[ENHANCEMENT] MAC filter - MAC address mask.</p>

	[eITS#230500277] CLI cfg command to IGMP snooping [eITS#230101253] From CLI, display remaining lease time on WAN ip lease
Mpro Mesh	[eITS#230101291] Disabling Mesh does not bring down the backhaul, which is still broadcasted as a hidden SSID [eITS#230300767] MProMesh App feature request to include guest isolation level
TR69	[eITS#230601075] XMPP / STUN server support [ENHANCE][ztr69cmd] Hide information about password.
TR369	[eITS#221000325] support TR369
Security	[Security] Setting Up the Password Strength [Security] disable console pin via software upgrade OpenSSL to 3.1.2
GUI	[eITS#230301802][GUI] Add connected LANport to client information [GUI] OPAL Generic Reboot Page Design
Wireless	[eITS#230600450] Wireless Network Max clients

## ● Bug Fixed

Modified Modules	Bug Fixed List
VoIP	[eITS#230701168]FXS Hook Status / Boot Check
Security	Zyxel-SI-1498 [Vulnerability] WPS vulnerability on CPE in WLAN [System] Wish description Protected Management Frames want to abbreviation, should change to PMF not show Protected MGMT Frames. [Security] Unauthenticated Access to APIs [Security] Session/Cookie Security Test [Security] Outdated Software [Security] Header Security Test [Vulnerability] Zyxel-SI-1506 [Vulnerability] Post-authentication buffer overflow Upgrade curl to 8.4.0

## Modifications in V5.18(ACHN.0)C0

Based on V5.18(ACHN.0)b6 to release V5.18(ACHN.0)C0

- Feature Enhancement
- Bug Fixed

## Modifications in V5.18(ACHN.0)b6

- Feature Enhancement
- Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	[#196500] [MPro Mesh] EX7501 Perform Mesh Full Factory Reset --- test failed

## Modifications in V5.18(ACHN.0)b5

- Feature Enhancement
- Bug Fixed

Modified Modules	Bug Fixed List
GUI	[GUI] Diagnostic page doesn't work. except Nslookup.

## Modifications in V5.18(ACHN.0)b4

- Feature Enhancement

Modified Modules	Features Enhancement List
Wi-Fi	[eITS #230501371] SSID naming logic when disabling mesh and allowing separate SSIDs

- Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	[MPro Mesh] AP_agent's beacon disapper after press WPS button.



GUI	[GUI] GUI will display "Backup WAN" page
WAN	<p>[WAN] After reboot / stress, Bridge WAN will inactive. need to apply again.</p> <p>[WAN] WAN LED will off when it link up with 5Gbps</p> <p>[WAN] use DS-Lite DHCP, LAN Client can NOT ping ipv4 (ex: 8.8.8.8) successfully</p> <p>[WAN] In GUI, PPPoE wan display IPoE wan's IPv6 address.</p>
System	<p>[System] GUI to change other language, some description will show English (ex: Dutch). Other(ex : title 、 options) will still show English, NAT &gt; PCP page always show English.</p> <p>[System] Sometimes Web GUI can not change to others page until refresh it</p>
Security	[Security] Parental Control typesetting issue
USB	[USB] Default admin account can't access security folder

## Modifications in V5.18(ACHN.0)b3

Modified Modules	Features Enhancement List
System	[eITS#221101418] OPAL, Partial factory reset option with firmware upgrades.
GUI	[OPAL Generic] GUI translation_ES_NL

### ● Bug Fixed

Modified Modules	Bug Fixed List
MPro Mesh	<p>[MPro Mesh_Android] When client run Internet Speed test, the Upload value always display 4.46Mbps.</p> <p>[MPro Mesh] Band steering test process controller does not have any 11v action records.</p>
Security	<p>[eITS#230500907] Possible security flaw that allows to retrieve root password.</p> <p>[Security] The subject is null after importing or creating certificate.</p>
GUI	[GUI] Parental control page display incorrect after add two

	<p>parental control rule.</p> <p>[GUI] Scheduler Rule time should display same as Parental control page.</p> <p>[GUI] In Maintenance &gt; Diagnostic, GUI display "Unknown Host or Unreachable Network!" after key in "www.google.com" and click Trace Route / Trace Route 6 / Nslookup.</p> <p>[System] Some words contain "@@" when the language is Español.</p> <p>[GUI] Some words contain "@@" when the language is Dutch or Türkçe.</p>
SNMP	[SNMP] Use SNMP to get CPE's description, but it does not match the description on CPE box.
TR-069	<p>[TR-069] CPE upgrade firmware from 0b1 to 0b2 via TR-069, but it will upgrade again after connecting to ACS.</p> <p>[TR-069] ACS GPV ['Device.DeviceInfo.Description'], but it does not match the description on CPE box.</p> <p>[TR-069] The value format of TR-069 cnonce not hexadecimal.</p>
VoIP	[VoIP] VoIP Region Setting not match with PS.
System	<p>[LED] When Ethernet LAN link speed is 5G, the 10G LAN LED cannot blink.</p> <p>[System] System Log/Security Log can't display correct time.</p>
WAN	<p>[WAN] In PPPoE mode with IPv6 only, CPE does not get IPv6 address after wan type change (ex: IPv4 only &lt;-&gt; IPv6 only). [fail rate: 60%(3/5)]</p> <p>[WAN] DS-Lite tunnel cannot be created when it's configured by DHCP automatically.</p> <p>[WAN] DS-Lite work fail with AFTR</p> <p>[WAN] In PPPoE modewith IPv4/v6 dual, CPE does not get IPv6 address after wan type change (IPv4/v6 &lt;-&gt; IPv4 only). [fail rate: 60%(3/5)]</p>

## Modifications in V5.18(ACHN.0)b2

### ● Feature Enhancement

Modified Modules	Features Enhancement List
------------------	---------------------------

System	[eITS #220901661] Configurable WiFi Country Code (ISO 3166-1 alpha-2) [eITS #220701077][System] [220701077] OPAL, Feature proposal/request - Soft-Reset feature [OPAL Regular] support APP 3.0 [ETSI EN 303 645] 5.3-2: When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.
TR-069	[eITS #230200423] TR-098 support for WiFi X_ZYXEL_CountryCode
MPro Mesh	[eITS #221000063] change the wording in SteerStatus
GUI	[eITS #220901550] Translation error WIFI password strength [eITS #221101418] OPAL, Partial factory reset option with firmware upgrades. (tr069/gui) 220701077 [GUI] Compact help link adding ito GUI
VoIP	[eITS #221101135][VoIP] SIP TLS encapsulation - supports SIP-over-TLS.
WAN	[eITS #230201111] iperf -R not implemented [eITS #230100744][eITS#230100744] bridge config improvement Interface grouping enhancement with TS enable for BCM solution
DHCP	[eITS #220900410] DHCP option providing CPE firmware version

## ● Bug Fixed

Modified Modules	Bug Fixed List
DNS	[eITS #230400106] DNSProxy issue when Primary DNS unreachable
TR-069	[eITS #230301653] CurrentTime not reporting in accordance to the TR-069 standard [eITS #230201161] enable/disable SSH via ACS [eITS #230300897] iPerf from tr069 fail, DownloadDiagnostics not ok, UploadDiagnostics ok [TR-181] Lifemote agent not work.

	<p>[TR-181] TR-069 Script execute cannot work.</p> <p>[TR-181] WiFi GUI not support WEP-64 and WEP-128 security mode but GPV include</p> <p>[eITS #230300429] certificate Common Name doesn't match host name</p>
GUI	<p>[eITS #230300494] GUI menu visible prior to login</p> <p>[GUI] Certificate option of TR-069 Client page can't display correctly.</p> <p>[eITS #230100382] Not possible too enable 5GHz WiFi in GUI, if WiFi first is turned off by physical button</p> <p>[GUI] In Security page, parental Control page does not logout GUI after Idle Timeout.</p> <p>[GUI] In Parental control page, PCP schedule time rule display incorrect when start time is empty.</p> <p>[GUI] In Parental control page, PCP schedule rule only display last schedule time when it create 3 schedule time rule.</p> <p>[GUI] LAN IPv6 prefix incorrect after Delegate prefix from WAN is change.</p> <p>[GUI] LAN PC login GUI fail with admin account. In console mode, login admin account without password. (test with production FW)</p> <p>[GUI] 10G LAN display 2.5G LAN on GUI</p> <p>[GUI] Connectivity page should display "Topology" and "list"</p> <p>CPE just will create one Static DHCP entry for STB Vendor ID devices</p>
Security	<p>[Security] GUI display duplicate Scheduler Rule rule.</p> <p>[Security] L2TP function work fail with more AP.</p> <p>[Security] L2TP function will disconnect after modify L2TP rule.</p>
WLAN	<p>[WLAN] WPS Method 2/3 should grayed out when use admin account.</p>
MPro Mesh	<p>[MPro Mesh_Agent] The wifi client's connection type show "Wired" in APP when clients connected guest wifi.</p> <p>[MPro Mesh] The "stale=Yes" scenario occurs during the AP roaming test.</p> <p>[MPro Mesh_Agent] After using "MPro Mesh" APP to logout or swipe up the screen to close it or enable wifi guest, it will</p>

	<p>always lead APP relogin fail.</p> <p>[MPro Mesh] RP Agent's GUI show wrong SSID after modify main or guest-1 SSID to special characters then turn on WIFI.</p> <p>[MPro Mesh_APP][ACTS] APP keep loading</p> <p>[MPro Mesh] After RP_Agent Onboarding and auto configure success, WX5600 Power LED light will twinkling again.</p> <p>[MPro Mesh] The online wifi client "stale" will be displayed as "Yes" during the AP roaming test</p> <p>[MPro Mesh] EX7501 disable mesh fail via CFG.</p> <p>[MPro Mesh] Agent's info disapper in connectivity page after on-boarding.</p>
MGMT	<p>[MGMT] MGMT remote page to enable SNMP WAN, CPE SNMP page function should not auto enable.</p> <p>[MGMT] Hide SSID of Guest/More AP of Wireless 2.4G and 5G can not be enabled via TR-069</p>
QoS	<p>[QoS] GUI will allow user to add a QoS queue with duplicate name "default queue"</p>
WAN	<p>[WAN] In PPPoE mode with IPv6 only, CPE does not get IPv6 address after wan type change (ex: IPv4 only &lt;-&gt; IPv6 only).</p> <p>[WAN] In System Monitor &gt; Log, click Refresh button then GUI will keep loading when CPE has PPPoE WAN.</p> <p>[WAN] PPPoE Passthrough cannot work</p> <p>[WAN] In PPPoE modewith IPv4/v6 dual, CPE does not get IPv6 address after wan type change (IPv4/v6 &lt;-&gt; IPv4 only).</p> <p>[WAN] LAN PC get new IPv6 prefix after click home networking page two times.</p> <p>[WAN] DUT cannot upgrade firmware via DHCP option 43 mechanism.</p> <p>[WAN] CPE not support MAP-E/MAP-T function.</p> <p>[WAN] CPE does not send release packet before CPE reboot.</p> <p>[WAN] In IPv4/v6 mode, CPE does not send release packet when click release button.</p> <p>[WAN] VLAN Auto-Hunt function work fail and LAN PC does not access GUI.</p>

System	<p>[System] System Log/Security Log can't display correct time.</p> <p>[System] CPE LAN LED will not Flickering, when traffic is ongoing</p> <p>[LED] LAN LED can NOT Flickering Green even there is traffic be transmitted.</p> <p>[System] after unplug/plug IPoE WAN cable, syslog can't not display on GUI</p> <p>[System] CPE does not match DST</p> <p>[System] CPE should support "Restore Partial Default Settings After Firmware Upgrade"</p> <p>[System] CPE should support "Partial Factory Reset"</p> <p>[System] after upload ROM file can't use GUI.</p> <p>[eITS #221200930]romd backup include option 125 devices specific option value</p> <p>[eITS #230101319]Lifemote trigger uncontrolled memory usage with script that is working for all other device types</p>
VoIP	<p>[VoIP] The Region Setting of VoIP that CPE supports are not match to PS</p> <p>[VoIP] When set Call Waiting Reject Timer of SIP Account to illegal value "empty", CPE should take correct values after pop warning message</p>
LAN	<p>[LAN] The photo of devices in Topology page should match to List page</p> <p>[LAN] RA packet that send from CPE LAN lack some option</p> <p>[LAN] Auto reserve IP for the same host works fail</p> <p>[LAN] When connect only one LAN Client to CPE and set Device Name of LAN Client to 64 characters, CPE cannot be display properly in the connectivity Topology page.</p> <p>[LAN] GUI display DHCP state is enable, but LAN PC can't get IP from CPE , LAN set static IP and it can not access internet (test with production FW)</p>
Wireless	[OPAL Generic] Max wireless clients limited to 32 pr band

## Modifications in V5.18(ACHN.0)b1

### ● Feature Enhancement

Modified Modules	Features Enhancement List
DHCP	[eITS #220900410]DHCP option providing CPE firmware version
DS-Lite	[eITS #221200506]Configuration of the AFTR should be possible with URL
System	Console redirect/Zconsole monitor [eITS #220301182]add possibility periodically reboot CPE using standard scheduler
GUI	[GUI] Compact help link adding ito GUI Networks Topology
Security	[ETSI EN 303 645] 5.8-2: The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage [ETSI EN 303 645] The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces
Http	Support Web http redirect to https.
Wifi	[eITS #210900469][OPAL Generic] Change WPS button trigger condition redmine, subnet configurable for TS enable

## ● Bug Fixed

Modified Modules	Bug Fixed List
GUI	warning message for IP conflict when TS enable
System	[eITS #230100138]rom-d backup
WAN	[eITS #221101734]No Management connection with new FW Version
Wifi	[eITS #220601144]WiFi button not working correct (behavior change)
Security	[CVE-2022-4203,4304,4450][CVE-2023-0215~0217,0286,0401][Zyxel-SI-1464] [Vulnerability] OpenSSL multiple vulnerabilities
TR-069	[eITS #221100865]TransferComplete messages without

	Start/Complete Time value [eITS #221200452]Activate IPV6 Default gateway by TR069 [eITS #220900371]NTP Time Server URL cannot support "-" [eITS #220401035][TR-069] SPV WiFi BeaconType failed [eITS #221101357]Issues with setting some parameters via TR069
ZYEE	[System]Refresh button in ZyEE Monitor page works fail [System] The Active and Idle button for EU cannot work