Firmware release notes of ValueLine Industrial Wireless devices

Affected models:

Device name	Article No.
IE-WL-VL-AP-BR-CL-EU	2536680000
IE-WLT-VL-AP-BR-CL-EU	2536690000
IE-WL-VL-AP-BR-CL-US	2536700000
IE-WLT-VL-AP-BR-CL-US	2536710000

Version 1.20.2 Build 25081511 (RED-DA compliant) — Released: September 2025

New Features:

- Added a firmware signature-verification mechanism.
- Added support for the Wi-Fi Auth/Assoc timeout setting.
- Added support for AP-Based Connection Management.
- Added support for Gratuitous ARP.
- Added support for Jumbo Frame (MTU).
- Added support for Wireless Link Health Check (AP).
- Support all channels and 11 channels for Client-based Turbo Roaming channel scanning.
- Added support for Wi-Fi Remote Connection Check.
- Added support for client isolation in AP mode.
- Added an option to allow the use of special characters.
- Added an option to configure password encryption.
- Added an option to configure the N multicast rate.
- Added an option to configure the HTTP/HTTPS web port.
- Function to enable/disable SSL Certificates
- Function to configure the 3rd SNMP trap receiver.
- Added an option to keep wireless enabled when resetting the IE-WL-VL-AP-BR-CL back to factory default settings.
- Added Indoor/outdoor channel list option.
- Added an option to show the PSK password in clear text.
- Web certificate support.
- Added an option to configure indoor/outdoor.

Enhancements:

- Added the CPU and memory usage SNMP node.
- Supports WLAN system log version 2.
- WPA supplicant supports TLS v1.2.
- Supports bridge status via SNMP.
- Devices will record a system log entry if an invalid configuration setting is reset to the default value.
- Enhance system stability.
- Enhance compatibility with other brands.

Bug Fixes/ Security Patches:

- [CVE-2023-52160] vulnerability.
- [CVE-2017-17562] vulnerability.
- Unauthenticated HTML/JS Injection (Stored XSS) into a web page.
- Simple bug fixes, security updates, and performance improvements.

Changes:

- Users are now required to change the default password when logging in to the web UI or CLI for the first time.
- Added a config check to ensure the UDP socket mode port range is set within 0 to 9999.
- Changed several names of SNMP OID.
- Changed the default multicast rate value according to the selected RF type.
- Changed the fixed rate list according to the selected RF type.
- Changed the management frame rate according to the selected RF type.
- Increased MAC/IP/Port filter entries up to 60.
- Adjusted the Wi-Fi signal level LED.
- The initial network IP is set to 169.254.0.1 before the DHCP server assigns an IP address for the first time.
- Changed the range for roaming threshold and AP candidate threshold from 5-40 to 5-60.
- Changed the UI field name "Signal Strength" to "Signal Level" on the wireless status page.
- The open "wireless interface" is now disabled by default.
- TELNET is now disabled by default.
- HTTP is disabled, and HTTPS is enabled by default.

Notes:

- This firmware is compliant with FOSS license requirements.
- This firmware complies with the EU RED-DA cybersecurity requirements (EN 18031-1:2024) related to RED Article 3.3(d) for products with connectivity functions that must prevent unauthorized access and misuse of data.
- For security reasons, a firmware signature mechanism was added to firmware v1.20.2. As a result, when uploading firmware in v1.20.2 or higher, you must upload a ZIP file that includes both the firmware file (.rom) and signature file (.sig). When upgrading to v1.20.2, you only need to upload the firmware file (.rom).

Version 1.11.13 Build 21010513 — Released: June 2021

Bug Fixes:

- Unable to establish a Wi-Fi connection with APs that support IEEE 802.11r

Security Patches:

- CVE-2021-33528: Improper system access as a higher privilege user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability
- CVE-2021-33529: Exploitable hard-coded cryptographic key allows for the decryption of captured traffic
- CVE-2021-33530/CVE-2021-33532/CVE-2021-33533/CVE-2021-33534: Improper Neutralization of special elements used in an OS command
- CVE-2021-33531: Exploitable hard-coded credentials
- CVE-2021-33535: Buffer copy without checking size of Inpup may cause remote code execution
- CVE-2021-33536: An attacker can send a crafted packet and cause denial-of-service of the device
- CVE-2021-33537: Stack-based buffer overflow
- CVE-2021-33538: Improper remote shell access to the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.
- CVE-2021-33539: An exploitable authentication bypass vulnerability. An attacker can trigger authentication bypass on specially configured device.

Version 1.11.10 Build 18122616 — Released: January 2020

Bug Fixes:

- Abnormal behaviour where DFS does not operate as expected
- Abnormal roaming handoff time if MAC clone enabled
- Device reboots if received abnormal beacon which format does not follow standard IEEE.
- Error handler for abnormal Wi-Fi packets does not work
- Static route of WLAN interface does not work if it applies DHCP client in Client-Router mode

Version 1.11.2 Build 18082313 Released: September 2018

Bug Fixes:

- Site Survey crashes after changing Operation Mode from Access Point to Client

New Features:

- Support for WDS-mode (Wireless Distribution System)
  Note: Limitations when using WDS-mode:
    - When selecting RF types G/N Mixed, B/G/N Mixed or A/N mixed mode, only N-mode can be effective.
    - WDS only supports security mode “open” or “WEP”, but N-mode doesn’t support WEP.
    - When “N mode” is configured as RF-type, then the security mode, using WDS, would be set to “Open”.
    - When WDS with “WEP” shall be used, RF-type must be set to B,G, B/G Mixed or A.

Version 1.9.2 Build 18030716 Released: April 2018

- First release