HiLCOS 10.12-RU7 released

2021-03-05 - Christoph Strauss - Wireless

Preface

HiLCOS is the operating system for the Hirschmann OpenBAT, BAT450, BAT450 11ac, BAT867 and BATWLC product. This document describes the innovations within HiLCOS software release 10.12 RU7, as well as the improvements since the previous version.

Known Issues

The use of RSTP together with AutoWDS can lead to an unstable AutoWDS network. It is recommended to use AutoWDS with RSTP disabled.

In very rare cases when adding a new Access Point (AP) in the AutoWDS network interactions between neighboring AutoWDS APs can occur. This can cause short-term disruptions of wireless links.

If APs are added in an AutoWDS network before enabling Auto-Accept, these APs must be accepted manually after switching Auto-Accept.

In rare cases the configuration rollout to a managed AP might take around 30 seconds longer when there is a configuration exchange in a redundant WLAN-Controller architecture.

Using the WLC redundancy feature access points do not re-distribute automatically to the preferred controller.

Broadcast attacks are invisible to the Wireless IDS.

An encrypted HiLCOS configuration, generated with HiLCOS 9.12, cannot be loaded in the current HiLCOS 10.12 release.

In rare cases the BAT867 health monitoring system may restart the device.

LANconfig can use SSH, TFTP, HTTP and HTTPS protocols to communicate with the devices. However due to changes regarding force password change, SSH cannot be used with

devices which still have a default password. As soon as the default password is changed on the device, SSH will start working normally.

Improvements in HiLCOS 10.12.6290-RU7

Bugfixes in HiLCOS 10.12-RU7

General

Update of Taiwan country profile according to NCC certification for BAT450-F devices:

o The following subbands are supported

- 2.4GHz band – channels 1-11 (20MHz) / 1-10 (40MHz)

- 5 GHz channels 36-48 and 149 -165

In previous versions of HiLCOS 10.12 it was not possible to reach a WAN interface from the WAN side. This issue is fixed with HiLCOS 10.12-RU7.

Several fixes regarding OpenSSL vulnerabilities are included to HiLCOS 10.12-RU7:

o EDIPARTYNAME NULL pointer de-reference (CVE-2020-1971)

o ECDSA remote timing attack (CVE-2019-1547)

o Fork Protection (CVE-2019-1549)

o Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

WLAN

In Malaysia country profile for 5GHz subband 3 the DFS-Channel Availability Check is disabled. This previously caused several minutes of delay until operation after powering up the device.

In previous versions of HiLCOS 10.12 the WiFi client address adaptation was not working correctly. This issue is fixed with HiLCOS 10.12-RU7.

When operating a BAT867 or BAT450-11ac device in client mode within a noisy environment

with several sources of interfering signals present, the device radio was in rare cases stopping communication. With HiLCOS 10.12-RU7 several improvement have been introduced to automatically recover from such cases.

Client devices roaming handover on BAT devices before HiLCOS 10.12-RU7 and HiLCOS 9.12-RU9 was impacted negatively by the following issues:

o In case of hidden and protected SSID the client was relying on probe response information only. Now the client also gets updated from beacons and outdated values are no longer taken into account. This leads to a better roaming decision.

o In case the handshake with the new AP is disrupted by interfering signals, the association might fail completely which can lead to a disruption longer than 5 seconds of the communication. In version HiLCOS 10.12-RU7 and HiLCOS 9.12-RU9 this issue is resolved.

Conteúdo relacionado

- HiLCOS-10.12.6290-RU7.zip