

Release Information

OWL Software Version 06.3.07

Copyright (c) 2002 – 2022 Hirschmann Automation and Control GmbH, Neckartenzlingen (Germany)

Hirschmann Automation and Control GmbH takes no responsibility or warranty for software not developed or manufactured by Hirschmann Automation and Control GmbH, especially with regard to shareware and other third-party software.

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Germany

Internet: <http://www.beldensolutions.com>

2022-11-29

Table of Contents

Preface	3
Initial Device Login	3
Known Issues	4
All OWLs	4
OWL LTE M12.....	4
OWL 4G	4
Note	5
All OWLs	5
OWL LTE M12.....	5
Valid software combinations	6
Software version 06.3.07	7
Added WiFi functions	7
Added VPN functions	8
Changes in default behavior and improvements to standard functions	9
Added general functions	13
Updates and security fixes	16
Software version 06.2.09	21
Software version 06.2.04	25
Software version 06.2.03	27
Software version 06.2.01	29
Software version 06.1.09	30
Software version 01.2.04 (2018-07-12)	33
Software version 01.2.03 (2018-02-19)	34
Software version 01.2.02 (2017-07-12)	34
Software version 01.2.01 (2017-01-06)	34
Comments	35

Preface

This document describes the innovations within the OWL software version 06.3.07.

Version 06.3.07 supports OWL 3G, OWL 4G, OWL LPWAN, OWL LTE and OWL LTE M12 devices.

Initial Device Login

Open the web interface of your OWL industrial cellular router device. **If you connect the first time to your device**, enter the default IP address 192.168.1.1/24 (on ETH0) in your web browser. The default username is **admin**. The default password for the admin user is printed on the router's label for OWL devices originally delivered with firmware version since 06.2.01. OWL devices originally delivered with firmware version 06.1.09 and lower have the default password **private**.

Prior to the Software update, backup the OWL configuration file with “Configuration” “Backup Configuration”. After that step, load the new OWL operating system into your device with “Configuration” “Software”

Known Issues

All OWLs

When using IPSec StrongSwan, only up to 2 of 4 tunnels can be used at the same time.

Changed default state:

OWL does no longer accept SMS by default: In case of an update from a previous release prior to 6.2.1 in a default state, there are no phone numbers configured so no SMS is accepted anymore. If the previous behaviour is still needed a "*" should be entered in the respective menu. Please check the configuration for that feature on the OWL, because between the different Software versions configurations are interpreted differently.

OWL LTE M12

The GPS chip of OWL LTE M12 includes Dead Reckoning. At the moment the GPS chip has the following limitations:

- 2-Dimensional Dead Reckoning only (altitude determination will be supported later)
- 1 Hz (10 Hz will be supported later)
- A-GPS only

OWL 4G

Country Code for WiFi

The first version of the firmware for the WiFi module does not support the settings of the country code. Due to this issue, the settings of the country code made on the configuration page has no effect at all. The country code is set up during the manufacturing process according to the product destination region.

WiFi Configuration – Lost After Firmware Downgrade

A Software downgrade to the version less than 6.2.0 resets the wifi configuration to the default again, which can then be configured later.

Note

All OWLs

Upgrading to the OWL software version 6.1.9 or higher requires upgrading the User Module GPS to version 1.6.9 to receive GPS coordinates. The order of upgrading the OWL software and the User Module GPS does not matter. The User Module GPS version 1.6.9 is not backward compatible with OWL software versions less than 6.1.9.

OWL LTE M12

During SIP/VoIP calls the LTE chip is set to 2G/3G. To get the best mobile communications technology available after a SIP/VoIP call has finished, select "Network Type = automatic selection" on the "Mobile WAN Configuration" dialogue.

When upgrading devices from older SW versions than 01.2.04, it is recommended to possibly upgrade the firmware on the LTE radio module. Please refer to the detailed instructions described in chapter "Software version 01.2.04 (2018-07-12)".

Valid software combinations

There are different types of software available for an OWL LTE M12. This document describes how they differ and what needs to be considered when upgrading and combining them. The types are:

- OWL firmware
- User Modules

The **OWL firmware** is the overall firmware that makes the OWL work. In addition to the web interface, it also contains the underlying Linux OS. The firmware file is named "OWL-LTE-M12.bin", the most recent version of this firmware is "6.2.9 (2021-04-07)".

The **User Modules** are like the apps on a smartphone, they are additional functions that are not included in the firmware and can be installed later. This can be done in the web-based menu "Customization -> User Modules". The files of the User Modules are normally tar- and zip-packed archives and named, for example, "gps.v3.tgz". They must not be unpacked for uploading.

To avoid complications, different combinations are tested. These tested combinations that work together are listed here:

OWL Firmware ↔ UM GPS

Firmware OWL LTE M12	GPS User Module
1.2.4 (2018-07-12) or below	GPS 1.3.4 (2017-03-28) or below
6.1.9 (2019-04-23)	GPS 1.6.4 (2019-03-27)
6.2.1 (2020-01-10)	GPS 1.6.6 (2019-11-13)
6.2.3 (2020-02-27)	GPS 1.6.9 (2020-01-27)
6.2.4 (2020-04-25)	
6.2.9 (2021-04-07)	
6.3.7 (2022-09-27)	GPS 1.10.0 (2021-09-21)

OWL Firmware ↔ UM SIP Gateway

Firmware OWL LTE M12	SIP Gateway User Module
1.2.4 (2018-07-12) or below	SIP Gateway 1.0.4 (2018-02-20)
6.1.9 (2019-04-23)	SIP Gateway 1.0.6 (2019-03-27)
6.2.1 (2020-01-10)	
6.2.3 (2020-02-27)	
6.2.4 (2020-04-25)	
6.2.9 (2021-04-07)	SIP Gateway 1.1.1 (2021-08-17)
6.3.7 (2022-09-27)	

OWL Firmware ↔ UM Self Phone Number

Firmware OWL LTE M12	Self Phone Number User Module
1.2.4 (2018-07-12) or below	Self Phone Number 1.0.1 (2017-09-25)
6.1.9 (2019-04-23)	
6.2.1 (2020-01-10)	
6.2.3 (2020-02-27)	
6.2.4 (2020-04-25)	
6.2.9 (2021-04-07)	Self Phone Number 1.2.0 (2020-10-01)
6.3.7 (2022-09-27)	

Software version 06.3.07

Added WiFi functions

Multi SSID Support

One of the main new features, implemented in this firmware, is support for two independent SSIDs for the WiFi AP mode. There are two independent configuration pages in the GUI called Access Point 1 and Access Point 2. Please note, that not all Hirschmann OWL routers support all the operation modes, APx & STA mode or AP1 & AP2 & STA mode. For more information see the Configuration Manual of your router.

WiFi WPA3 Support

Starting with this firmware release, we have added support for the new WPA-3 WiFi authentication. This option is available for both Access Point and Station mode configuration. WiFi protected Access 3 (WPA3) is the next-generation WiFi encryption protocol. WPA3 builds upon trusted WPA2 success to bring a new level of security for personal and enterprise environments.

SSID Isolation

There is a new option in the WiFi Access Point configuration, enabling the SSID Isolation feature. When enabled, a WiFi client connected to the Access Point cannot communicate with another WiFi client connected to another Access Point. However, this client can still communicate with a client connected to the same Access Point unless the Client Isolation is not enabled.

WiFi Firmware and Driver Update

We have updated the firmware of the Laird SU60 WiFi module to version 5.5.38.5. Moreover, the module driver was updated to the version 8.5.0.7.

Updated wpa_supplicant Program

We have updated the wpa_supplicant program to version 2.10. This update has fixed CVE-2022-23303 (critical) and CVE-2022-23304 (critical). For more details about this release, see the webpage at https://w1.fi/cgit/hostap/plain/wpa_supplicant/ChangeLog.

Updated hostapd Program

We have updated the hostapd program to version 2.10. This update has fixed CVE-2022-23303 (critical) and CVE-2022-23304 (critical). For more details about this release, see the webpage at <https://w1.fi/cgit/hostap/plain/hostapd/ChangeLog>.

Updated libnl Program

We have updated the libnl program to version 3.2.25 due to the upgrade of hostapd and wpa_supplicant programs. For more details about this release, see the webpage at <https://www.infradead.org/~tgr/libnl/>.

Added VPN functions

Route-based VPN Support

We have made a significant enhancement of the IPsec functionality in this firmware release. The route-based VPN policy is now supported. So both, policy-based and route-based VPN approaches are supported by Hirschmann OWL routers. See the router's Configuration Manual and IPSEC tunnel for more information about the IPsec configuration.

IPsec Certificate-chain Validation

We have added support for the certificate-chain based validation to the IPsec tunnel functionality. In the IPsec configuration, users may define a CA certificate without specifying a remote peer certificate. This will accept all peers with certificates signed by this CA.

Upgraded IPsec Configuration File

We have upgraded the IPsec configuration file to a new format named swanctl.conf. A user script, working directly with the IPsec configuration file, may be affected by this change. See the Migration from ipsec.conf to swanctl.conf strongSwan web page for detailed information.

WireGuard VPN Support

WireGuard is a communication protocol and free open-source software that implements encrypted virtual private networks (VPNs) and is designed with the goals of ease usage, high speed performance, and low attack surface. It aims for better performance and more power than IPsec and OpenVPN, two common tunneling protocols. The WireGuard protocol passes traffic over UDP. Hirschmann OWL routers now support up to four WireGuard tunnel configurations. For more information, see the Configuration Manual of your router.

Cisco FlexVPN Support

We have added support for the Cisco FlexVPN. Internet Key Exchange Version 2 (IKEv2), a next-generation key management protocol based on RFC 4306, is an enhancement of the IKE Protocol. IKEv2 is used for performing mutual authentication and establishing and maintaining security associations (SAs). FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site-to-site, remote access, hub-and-spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using crypto maps. To enable the Cisco FlexVPN feature, enable the Cisco FlexVPN on the IPsec configuration page.

IPsec Configuration Enhancement

We have made several configuration enhancements to the IPsec configuration in the GUI so that the following items can be now configured:

- 2nd Remote IP Address entry for the second remote IP address.
- MTU (Maximum Transmission Unit) entry (for route-based mode only).
- User's Up/Down Scripts that are executed when the IPsec tunnel is established/closed.

OpenVPN Configuration Enhancement

We have made several configuration enhancements to the OpenVPN configuration in the GUI so that users can now configure the following items:

- 2nd Remote IP Address entry for the second remote IP address.
- Local Passphrase entry.
- Username and Password authentication can be used for relevant authentication modes.
- User's Up/Down Scripts that are executed when the OpenVPN tunnel is established/closed.

OpenVPN TAP Support

In addition to TUN mode, OpenVPN now also supports TAP mode. TAP is basically at the Ethernet level (layer 2) and acts as a switch, whereas TUN works at the network level (layer 3) and routes packets on the VPN. TAP is bridging, whereas TUN is routing. To configure the TAP mode, configure the bridge on ethernet interface first and then choose this mode in OpenVPN configuration, field Interface Type.

IPsec Asymmetric PSK

Asymmetric PSK for IPsec configuration is supported now. It allows establishing an IKEv2 VPN with an asymmetric Pre-Share key between two routers. It can be used when establishing the IPsec tunnel to a CISCO router. On an Hirschmann OWL router, set the IPsec Authenticate Mode to the pre-shared key, IKE Protocol to IKEv2, and set up the Pre-shared Key together with the Remote Pre-shared key. For more information, see the IPsec Tunnel application note and Configuration Manual of your router.

Updated OpenVPN Software

We have updated the OpenVPN software to version 2.4.12. This update has fixed CVE-2022-0547 (critical). For more details about this release, see the webpage at <https://github.com/OpenVPN/openvpn/blob/release/2.4/Changes.rst>, chapter Version 2.4.12.

Changes in default behavior and improvements to standard functions

Updated Syslog Format

Format of the syslog message, which is sent to the external network output, was changed to meet the RFC 3164 standard. Now, each message has a facility and severity code assigned. The new format enables integration with external log monitoring tools allowing to react in significant events, such as an authentication failure is. Note that the textual output in the router GUI remains not affected by this update. Here is an example of the new message format, starting with the facility and severity number: Jul 27 13:41:29 https: user 'root' logged in from 192.168.1.1

SMS Configuration Enhancement

There is a new BIN1 - SMS option in the SMS configuration page. The SMS message text, to be sent when the second binary input is activated, can be configured here.

PPTP Configuration Enhancement

There are two new options in the PPTP configuration page available to configure the MTU (Maximum Transmission Unit) and the MRU (Maximum Receive Unit) parameters. The default value for both options is 1460 bytes to avoid sending fragmented packets.

L2TP Configuration Enhancement

There are two new options in the L2TP configuration page available to configure the MTU (Maximum Transmission Unit) and the MRU (Maximum Receive Unit) parameters. The default value for both options is 1400 bytes, the same as used so far.

Signal Strength Indication Improvement

Cellular signal strength, reported on the Mobile WAN status page, was enhanced with a new field for SINR value. This parameter is available in the SNMP mobile subtree as well.

Changed RST Button Behavior

For the router's factory reset, when the RST button is held for more than four seconds, the reset is performed when the button is released. Originally, the reset was performed four seconds after the button was pressed.

LAN GUI Menu Renamed

We have changed the name for the Ethernet interfaces in the GUI. The menu item changed from LAN to Ethernet and the sub-menus from Primary LAN to ETH0, Secondary LAN to ETH1, etc.

Location and Name in GUI

Location and Name are now always visible in the top right corner of the GUI, not only when configured. If not configured, the "N/A" text is displayed here instead. You can enter both these entries in the Services -> SNMP configuration menu.

SSH Key Regenerating

The OpenSSH software does not support the private keys of 512 bits length since version 7.6. Therefore, we have added support for the manual SSH key regeneration to the increased key length.

Welcome Page Redirecting

If there is a welcome page in any installed Router App (User Module), the router redirects the logged user to this page after successful web login. Note that the welcome page filename should be welcome.cgi. If more Router Apps have the welcome page installed, the first found page is displayed.

Web Session Invalidation

After the user password change, all the opened web sessions are invalidated for that user account.

System Log Storage

There is a new function of persistent system log storage. If enabled, the log is stored in the file located in non-volatile memory, so it is not lost after restarting or shutting down the router. It can be enabled in the GUI (Configuration -> Services -> Syslog -> Log Persistent) and is supported by routers having the eMMC memory only.

Syslog Remote Device ID

The router identification string, used for the remote sys logging, can now be specified in the Configuration -> Services -> Syslog -> Device ID field. This feature may be handy if more routers log into one remote server. If the Device ID parameter is not specified, the default string Router is used.

Renamed User Modules Menu Item

Hirschmann OWL routers support custom software programs to enhance the router's features. Since these applications were renamed from User Modules to Router Apps some time ago, there is also a corresponding renaming in the router GUI. The Customization -> User Modules menu item was renamed to the Customization -> Router Apps.

Live Data in GUI

All status pages of the web interface can now display live data. To enable this feature, click on the refresh button in the top right corner of one of the status pages. To stop the data update and to limit the amount of data transferred, disable automatic data updates by clicking the pause button again.

Added HTTP and SSH Login Banner

There is a new configuration field called Login Banner in the HTTP and SSH configuration pages. The text specified within this optional field is displayed on the HTTP login page respectively in the console when login in by SSH.

Unprivileged Mode

Some network services now run in the unprivileged mode having restricted access to system resources. We have made this measure due to security reasons.

Enabled HSTS Policy

We have added the HSTS (HTTP Strict Transport Security) header to the HTTPS responses in case the HTTP access is disabled in the configuration. This security measure will prevent the downgrade of HTTPS protocol to HTTP protocol. To work correctly, a certificate signed by a certification authority must be uploaded and a domain account must be used for router logging.

Disabled Obsolete TLS Versions

The TLS (Transport Layer Security) versions 1.0 and TLS 1.1 are now disabled in the default configuration. Using versions lower than 1.2 is unsafe and, therefore, not recommended. In the future, the use of these versions will be prohibited.

Configuration Parameter Length Lifted

We have removed the limitation of configuration parameter length that could be passed to an application in the console. The length of parameters was limited to 8 KB until now.

Enabled PIE Generation

We have enabled the generation of position-independent executables (PIE) for all affected router platforms. Position Independent Executables can be loaded anywhere in memory, much like shared libraries. This method increases the security of executable files.

Session Cookie Configuration

The session ID cookie is now protected with the Secure, HttpOnly, and SameSite=Strict attributes.

Added general functions

TAC in Mobile WAN Status

The LAC (Location Area Code) information, reported on the Mobile WAN status page, is now replaced by the TAC (Tracking Area Code) in case the of the LTE and 5G cellular network. The same rule applies for the status command.

Updated Syslog Format

Format of the syslog message, which is sent to the external network output, was changed to meet the RFC 3164 standard. Now, each message has a facility and severity code assigned. The new format enables integration with external log monitoring tools allowing to react in significant events, such as an authentication failure is. Note that the textual output in the router GUI remains no affected by this update.

Here is an example of the new message format, starting with the facility and severity number:

Jul 27 13:41:29 https: user 'root' logged in from 192.168.1.1

SMS Configuration Enhancement

There is a new BIN1 - SMS option in the SMS configuration page. The SMS message text, to be sent when the second binary input is activated, can be configured here.

PPTP Configuration Enhancement

There are two new options in the PPTP configuration page available to configure the MTU (Maximum Transmission Unit) and the MRU (Maximum Receive Unit) parameters. The default value for both options is 1460 bytes to avoid sending fragmented packets.

L2TP Configuration Enhancement

There are two new options in the L2TP configuration page available to configure the MTU (Maximum Transmission Unit) and the MRU (Maximum Receive Unit) parameters. The default value for both options is 1400 bytes, the same as used so far.

Signal Strength Indication Improvement

Cellular signal strength, reported on the Mobile WAN status page, was enhanced with a new field for SINR value. This parameter is available in the SNMP mobile subtree as well.

Changed RST Button Behavior

For the router's factory reset, when the RST button is held for more than four seconds, the reset is performed when the button is released. Originally, the reset was performed four seconds after the button was pressed.

LAN GUI Menu Renamed

We have changed the name for the Ethernet interfaces in the GUI. The menu item changed from LAN to Ethernet and the sub-menus from Primary LAN to ETH0, Secondary LAN to ETH1, etc.

Location and Name in GUI

Location and Name are now always visible in the top right corner of the GUI, not only when configured. If not configured, the "N/A" text is displayed here instead. You can enter both these entries in the Services -> SNMP configuration menu.

Enabled MTU Discovery

We have enabled the automatic MTU discovery feature for the cellular network, which may decrease the MTU value. This update will fix a communication issue in networks not supporting the default MTU 1500 bytes.

Changed GRE TTL

The TTL for the GRE packet was set to a fixed value of 64 bytes. This solution will prevent issues with the GRE tunnel in some specific scenarios.

Ethernet MTU Setting

We have added support for setting the MTU (Maximum Transmission Unit) for the Ethernet interfaces.

SSH Key Regenerating

The OpenSSH software does not support the private keys of 512 bits length since version 7.6. Therefore, we have added support for the manual SSH key regeneration to the increased key length.

Welcome Page Redirecting

If there is a welcome page in any installed Router App (User Module), the router redirects the logged user to this page after successful web login. Note that the welcome page filename should be welcome.cgi. If more Router Apps have the welcome page installed, the first found page is displayed.

New iptables Extension

The u32 match extension is now supported by the iptables. This module allows the matching of arbitrary bytes in a packet. Visit the u32 tutorial page for a detailed description of this match extension.

Firewall Rules Increased

The total amount of the firewall rules, that can be configured on the Firewall configuration page, was increased from eight to sixteen rules for both, the incoming and forwarded packets.

Docker Support

This firmware release contains updates to support the new Docker Router App supporting the Docker platform for the Hirschmann OWL routers. Docker is an open platform for developing, shipping, and running applications. Docker provides the ability to package and run an application in a loosely isolated environment called a container. A Docker container image is a lightweight, standalone, executable

package of software that includes everything needed to run an application: code, runtime, system tools, system libraries, and settings. See docker.com for the platform homepage or hub.docker.com for the container images repository. Note: Models equipped with built-in eMMC memory are required to support the Docker Router App.

SNMP Enhancement

SNMP information for cellular band number, signal strength, CPU usage, and RAM usage is now available. See the SNMP Object Identifiers application note for detailed information.

Added shred Program

We have added support for the shred program, which can delete a file from non-volatile memory entirely. This command overwrites the contents of a file multiple times, using patterns chosen to maximize the destruction of the residual data, making it harder for even costly hardware probing to recover it. See the Commands and Scripts application note for detailed information about this command.

Added sysctl Program

We have added support for the sysctl program, which can list and modify kernel parameters at runtime. The parameters available are those listed under `/proc/sys/`. Check the Commands and Scripts application note for more information about this program.

New iptables Extension

Added support for the addrtype match extension to the iptables utility. This module matches packets based on their address type. Address types are used within the kernel networking stack and categorize addresses into various groups. Visit Addrtype match manual page for a detailed description of match extension or iptables manual pages eventually.

New ebtables Extension

Added support for the mark match extensions to the ebtables utility. The mark extension matches packets based on the marks they have set. For more information about ebtables, see the ebtables manual page.

SFTP File Access Logging

As a security enhancement, the SFTP configuration was changed to log the SFTP level file access.

Two-factor Authentication Support

We have made the required updates to allow customers to use two-factor authentication. Currently supported third-party solutions supporting the Linux PAM are Google Authenticator and OATH Toolkit. For more information, see the Configuration Manual of your router, chapter Administration -> Two-Factor Authentication.

Web Session Invalidation

After the user password change, all the opened web sessions are invalidated for that user account.

Added dd Program

We have added support for the dd program, which can be used to copy a file and convert the data format in the process, according to the operands specified. See the Commands and Scripts application note for detailed information about this command.

Added HTTP and SSH Login Banner

There is a new configuration field called Login Banner in the HTTP and SSH configuration pages. The text specified within this optional field is displayed on the HTTP login page respectively in the console when login in by SSH.

License List Enhancement

The licenses list, which can be opened by the Licenses link under Status -> General -> System Information page, was enhanced with the package's version. The list is split into Bootloader and Firmware sections. In addition, this license list now supports displaying the installed Router Apps licenses, if supported by the Router App.

Enhanced gsmat Program

The gsmat is a program that can send an AT command to the cellular module. This command now supports the timeout option, as shown in the syntax below. Note that the default timeout remains 10 seconds.

Syntax: gsmat [-t <timeout>] <AT command>

Updates and security fixes

Security Improvements

We have applied various kernel and userspace hardening techniques as a security enhancement. Some of the most significant improvements are:

- Enabled hardening of common str/mem functions in 1st party binaries.
- Enabled hardening of str/mem functions in Linux kernel.
- Enabled generating of position-independent code in 1st party binaries.
- Disabled /dev/mem device.
- Restricted dmesg access.
- Enabled strong stack protector in Linux kernel.
- Enabled hardening of memory copies between userspace and Linux kernel.
- Enabled PAN emulation in Linux kernel.
- Enabled Yama Linux Security Module.

General Security Fixes

We have fixed CVE-2022-37434 (critical) in zlib library.

TCP Fix Applied

We have enabled the protection against the TCP TIME-WAIT assassination hazard. See the RFC 1337 for more details.

OpenSSL Security Fix

For security reasons, the compression and deprecated ciphers in OpenSSL were disabled.

HTTP Security Headers

New HTTP security headers Content-Security-Policy, Referrer-Policy, and Permissions-Policy were added to protect the HTTP against various attacks.

GPRS Connection Fix

We have fixed an issue with the GPRS connection on Telit LE910-EU V2 cellular modules with firmware 20.00.406.

AT&T 3G Sunset Fix

We have changed the cellular module's configuration to work in LTE networks once the AT&T 3G shuts down as planned by February 22nd, 2022. The cellular modules were configured to be data-centric instead of voice-centric.

IPsec Security Improvement

We have improved the interoperability and security of IPsec by adding the default ciphers to the IKE and ESP proposals.

IPsec Configuration Fix

We had fixed an IPsec malfunction issue when the PFS was enabled and the ESP Algorithm was set to auto.

Fixed Linux Kernel Vulnerabilities

This update has fixed CVE-2020-24586 (low), CVE-2020-24587 (low), CVE-2020-24588 (low), CVE-2020-26139 (medium), CVE-2020-26147 (medium), CVE-2020-26558 (medium), CVE-2020-36386 (high), CVE-2021-20322 (N/A), CVE-2021-45485 (high), CVE-2022-1012 (critical), CVE-2022-32296 (low), CVE-2022-36946 (high), CVE-2022-20368 (high). and CVE-2021-45486(low) in the Linux kernel.

Fixed RS232 Communication

We have fixed an issue with the broken RS232 hardware flow control.

Fixed IPsec Issue

We have fixed the issue for route-based IPsec. If the responder's remote IP address was within the remote subnet, the router lost remote access to the device via (M)WAN.

Fixed Possible XSS Attack

We have fixed the possible reflected XSS attack when a malicious code could be executed in the web browser. The router itself is not affected by this vulnerability.

Fix for snmptrap Program

We have fixed the snmptrap program to exit with code 1 if sending an SNMP has failed.

Fixed USB and DMA Drivers Issues

We have fixed several USB and DMA drivers issues by backporting the fixes from the kernel version 4.14.250.

Fixed I2C Driver Issues

We have fixed several I2C driver issues. These issues may get the router into a state when it cannot start up at all.

Fixed Localhost Resolving

We have made a fix to allow the loopback IP address to resolve the localhost hostname.

Fixed IPv6 Scripts Backup

We have fixed an issue with the backup of the IPv6 up/down scripts during the router's firmware update. Files /etc/scripts/ip6-up.local and /etc/scripts/ip6-down.local are not backed up and restored properly.

Mobile Connection Fix

We have applied a fix for connection to a mobile network in IPv6-only mode.

Improved DHCP Server Status

The DHCP server status reported in the GUI was redesigned to make it more transparent. The basic information about DHCP leases is now displayed in a table with a few columns.

Fixed ICMPv6 Ping over PPPoE

We have fixed sending of ICMPv6 ping over the PPPoE interface. This issue may cause an IPv6 route to be missing in the routing table.

Resolved WiFi Freezing

We have fixed occasional WiFi module freezing during the AP network searching.

Fix for ip Program

We have fixed the VLAN/VRF ID listing by ip program. This issue caused an incorrect VLAN/VRF ID to be printed by the program.

Fixed MAC Resolving

We had resolved a bug in the IPv6 MAC address resolving function that occurred when many addresses were logged.

Fixed VRRP Service

We have fixed the occasional crashing of the VRRP (Virtual Router Redundancy Protocol) service.

IPsec/OpenVPN Script Fix

We have fixed the calling of IPsec and OpenVPN up/down scripts in alternative profiles.

Replaced ndppd Library

We have replaced the ndppd library, software to support proxy NDP packets, with the ndp proxy library. We have made this replacement to reduce the size occupied by this software.

Replaced inetutils Software

We have replaced inetutils software, a collection of network programs, with Pure-FTPd software to support an FTP server functionality. The rationale for this replacement was to reduce the required system resources and provide the required security. For more details about this software, see the Pure-FTPd webpage.

Updated OpenSSH Software

We have updated the OpenSSH software to version 8.8p1. This update has fixed CVE-2020- 14145 (medium) and CVE-2020-15778 (high). Further is has fixed CVE-2016-20012 (medium) and CVE-2021-41617 (high). For more details about this release, see the webpage at <https://www.openssh.com/releasenotes.html>.

Updated OpenVPN Software

We have updated the OpenVPN software to version 2.4.11. This update has fixed CVE-2020- 15078. For more details about this release, see the webpage at [https://openvpn.net/ community-downloads/](https://openvpn.net/community-downloads/).

Updated dnsmasq Software

We have updated the dnsmasq software to version 2.85. This update has fixed CVE-2021-3448 (medium). For more details about this release, see the webpage at <http://www.thekelleys.org.uk/dnsmasq/CHANGELOG> .

Updated StrongSwan Software

We have updated the strongSwan software to version 5.9.6. This update has improved the Denial of Service (DoS) protection. Further, this update has fixed CVE-2021-41990 (high), CVE-2021-41991 (high). For more details about this release, see the strongSwan 5.9.6 Changelog.

Updated dhcp-isc Software

We have updated the dhcp-isc program to version 4.1-ESV-R16-P1. This update has fixed CVE-2021-25217 (high). For more details about this release, see the webpage at <https://downloads.isc.org/isc/dhcp/4.1-ESV-R16-P1/dhcp-4.1-ESV-R16-P1-RELNOTES>.

Updated curl Program

We have updated the curl program to version 7.84.0. This update has fixed CVE-2021-22897 (medium), CVE-2021-22898 (low), CVE-2021-22901 (high), CVE-2021-22922, CVE-2021-22923, CVE-2021-22924, CVE-2021-22925, CVE-2021-22926,, CVE-2021-22945, CVE-2021-22946, CVE-2021-22947, CVE-2022-27778 (high), CVE-2022-27779 (medium), CVE-2022-27780 (high), CVE-2022-27781 (high), CVE-2022-27782 (high), CVE-2022-30115 (medium). CVE-2022-32205 (medium), CVE-2022-32206 (medium), CVE-2022-32207 (critical), CVE-2022-32208 (medium), and CVE-2022-35252 (N/A). For more details about this release, see the Curl Changelog webpage.

Updated OpenSSL Library

We have updated the OpenSSL library to version 1.1.1q This update has fixed CVE-2021- 3711 (critical), CVE-2021-3712 (high), CVE-2022-0778 (high). CVE-2022-1292

(critical) and CVE-2022-2068 (critical). For more details about this release, see the OpenSSL Changes webpage.

Updated glibc Library

We have updated the Glibc library to version 2.35. This update has fixed CVE-2010-4756 (N/A), CVE-2019-25013 (medium), CVE-2019-1010022 (critical), CVE-2019-1010024 (medium), CVE-2019-1010025 (medium), CVE-2020-1752 (high), CVE-2020-6096 (high), CVE-2020-10029 (medium), CVE-2020-27618 (medium), CVE-2020-29562 (medium), CVE-2021-3326 (high), CVE-2021-35942 (critical), CVE-2022-23218 (critical), and CVE-2022-23219 (critical). For more details about this release, see the GNU C Library version 2.35 webpage.

Upgraded BusyBox Software

The BusyBox software suite was upgraded to version 1.34.1. This update has fixed CVE-2022-28391 (high). Many further changes, including many security fixes, have been made, see the webpage at <https://busybox.net/news.html>.

Updated ppp Program

We have updated the ppp program to version 2.4.9. This update has fixed CVE-2020-8597(critical) and CVE-2015-3310 (N/A). For more details about this program, see the webpage at <https://launchpad.net/debian/+source/ppp/+changelog>.

Upgraded zlib library

We have updated the zlib library to version 1.2.12. This update has fixed CVE-2018-25032.(high). For more details about this release, see the webpage at <https://www.zlib.net/>.

Updated Net-SNMP Software

We have updated the Net-SNMP software to version 5.9.3. This update has fixed various issues in version 5.8, including an occasional crash when reading values using the SNMP GETBULK command. Further, this update has fixed CVE-2022-24805 (N/A), CVE-2022-24806 (N/A), CVE-2022-24807 (N/A), CVE-2022-24808 (N/A), CVE-2022-24809 (N/A), and CVE-2022-24810 (N/A).

Software version 06.2.09

Changed Password Encryption

We have changed the password encryption method from MD5 to a more secure SHA256 method. Please note that an existing password is stored with original encryption until it is updated.

Configuration File Parameters

The maximum number of parameters in a configuration file was increased from 200 to 1000. This allows a user module to store even more parameters to the configuration file.

Disabled Password Auto-completion

Fixed password input fields in the change password menu. Browsers now correctly hide the password when typing and auto-completion is disabled.

Fixed Linux Kernel Vulnerability

This update has fixed CVE-2019-19447 (medium) in the Linux kernel.

Updated StrongSwan Software

We have updated the StrongSwan software to version 5.8.4.

Firewall and NAT Description

On the Firewall and NAT configurations GUI, a description can be added to each entry.

Fixed SNMP Service Restart

We have fixed a rare issue that may occur when restarting the SNMP service. This issue was caused by starting a new instance of snmpd service while the old one is still running.

VRF Lite Support

Support of Virtual Routing and Forwarding (VRF) Lite in Linux kernel was enabled. For more details about the VRF, see the webpage at <https://www.kernel.org/doc/Documentation/networking/vrf.txt>.

Expansion Ports Commands

We have added two new commands to the CLI to control the expansion ports. These programs are port1 and port2, the port1 command controls the first expansion port, the port2 command controls the second expansion port. The syntax for both commands is described below.

Synopsis:

```
port1 [on|off|auto|rs232|rs485]
port2 [on|off|auto|rs232|rs485]
```

Options:

Option	Description
on	Turn on the expansion port.
off	Turn off the expansion port.
auto	Turn on the expansion port and set the flow control (CTS signal) to RS232 or RS485 mode depending on the type of the expansion board.
rs232	Turn on the expansion port and set the flow control (CTS signal) to RS232 mode.
rs485	Turn on the expansion port and set the flow control (CTS signal) to RS485 mode.

User Authentication Logging

We have added logging of unsuccessful web login events into the syslog, for security and monitoring purposes.

Commands Permission Check

A strict permission check is now performed when running a command requiring the administration (root) permission. This type of command is not executed anymore, instead the permission denied error message is returned. This fix will eliminate a confusion with incorrect command output, for a command requiring the administration permission, such as `status`, `report`, `gsmat`, `io`, etc., if executed without the administration permission.

POSIX Message Queues Support

We have enabled the POSIX message queues in the Linux kernel, so it can be used by a user module. POSIX message queues allow processes to exchange data in the form of messages. For more information see `mq_overview` manual page.

Fixed Key File Importing

We have fixed an issue with importing an encrypted private key file when the file content was not processed correctly.

Fixed Linux Kernel Vulnerabilities

This update has fixed CVE-2020-10135 (medium), CVE-2020-12351 (high), CVE-2020-12352 (medium), CVE-2020-24490 (high) and CVE-2020-25705 (high) in the Linux kernel.

Updated TACACS+ Module

We have updated the TACACS+ authentication PAM module to version 1.6.1. This update has fixed CVE-2020-27743 (critical) and CVE-2020-13881 (high).

Updated OpenVPN Software

We have updated the OpenVPN software to version 2.4.10. For more details about this release, see the webpage at <https://openvpn.net/community-downloads/>.

Enhanced OpenVPN Configuration

There is a new configuration option Security Mode in the OpenVPN configuration GUI. Here, for relevant authentication modes only, you can choose from two different security modes `tls-auth` and `tls-crypt`. We recommend using the `tls-crypt` mode for security reasons. In this mode, all the data is encrypted with a pre-shared key. Moreover, this mode is more robust against the TLS denial of service attacks.

Enhanced GRE Configuration

We have enhanced the GRE tunnel configuration GUI with the local IP address configuration option. This item is optional together with a remote IP address and pre-shared key, but at least one of them must be configured.

HTTPS TLS Version Configuration

A minimal version of TLS protocol can now be configured in HTTP GUI settings to version 1.3. We recommend using the latest version of TLS. Support for other versions persists due to compatibility with various web browsers.

Added doas Program

There is a new program called `doas` which can be used to execute commands as another user. This program replaces the `sudo` command, which is not supported by the firmware from version 6.2.8 anymore. For compatibility reasons, the `sudo` command is just a symlink to the `doas` command. Check the Commands and Scripts application note for more information about this program.

Out-of-memory Reboot

We have changed the settings of the out-of-memory feature. It will now invoke the kernel panics compulsorily and reboot the router with no processes killed by the out-of-memory killer.

DHCP Authoritative Mode

Configuration of the DHCP server, running on our routers, was updated to act as the authoritative DHCP server for all WiFi clients. Authoritative DHCP server is a server that always responds to a DHCP request if no other DHCP server in the network responds. This configuration prevents an issue with obtaining the IP address for some WiFi clients having a valid address assigned in another WiFi network.

Fixed WiFi Issue

We have made a fix for transmitting issues on the OWL 4G + WLAN products. This issue caused the WiFi to stop working. If required, this fix will invoke a reboot of the router.

Fixed OpenVPN Issue

We have fixed an issue with resolving of IP address in OpenVPN version 2.4. The OpenVPN configuration was updated to be compatible with OpenVPN of version 2.3.

Fixed Possible XSS Attack

We have fixed possible reflected XSS attack (medium severity) in the web administration.

Updated curl Program

We have updated the curl program to version 7.76.0. This update has fixed CVE-2021-22876 (medium) and CVE-2021-22890 (low). For more details about this curl release, see https://curl.haxx.se/changes.html#7_76_0.

Updated dnsmasq Software

We have updated the dnsmasq software to version 2.84. This update has fixed CVE-2020-25681, CVE-2020-25682 (high), CVE-2020-25683, CVE-2020-25687 (medium), CVE-2020-25684, CVE-2020-25685 and CVE-2020-25686 (low). For more details about the release, see the webpage at <http://www.thekelleys.org.uk/dnsmasq/CHANGELOG>.

Mobile WAN Status Enhancement

Information reported on the Mobile WAN status page was enhanced with new fields for RSSI, RSRP, RSRQ, RSCP, Ec/Io and the frequency band number. Please note, that some of this information may not be displayed, if not supported by the cellular module.

Identity Validation

There are some special characters, “ \$ & ' () ; < > \ ^ ' | ”, which are not allowed to be used for some types of identity fields in the GUI. This restriction is implemented to most of the username, password, or other identity fields. What the function did, was that it removed all the forbidden characters during the data storage without a warning message. It could be confusing, especially for forms with hidden characters, typically for the password entry. From now, a warning message pops up, informing that an invalid entry was entered, and the form storage is not allowed.

New Programs Supported

There are six new programs supported by the firmware, see the table below. For detailed information about these commands, please see the “Commands and Scripts” application note.

Program	Description
basename	Strips directory path and suffix from the file.
cut	Prints selected fields from each input file to standard output.
dirname	Strips non-directory suffix from filename.
printf	Formats and prints argument(s) according to the specified format (as in C).
readlink	Displays the value of a symlink.
realpath	Returns the absolute pathname of the given file name.

New Default APNs

We have added these default APNs:

- For PLMN 22603 set up to the broadband string.
- For PLMN 22610 set up to the net string.

Updated OpenSSL Library

We have updated the OpenSSL library to version 1.1.1k. This update has fixed CVE-2021-3449 (medium) and CVE-2021-3450 (high).

Updated FTP Service

We have updated the FTP service (program ftpd) in the firmware to version 2.0. This update has fixed a stack overflow vulnerability (in the client-side environment) together with possible buffer overflow vulnerability.

Software version 06.2.04

SHA384 Support for IPsec

Secure hash algorithm SHA384 is now supported by the IPsec. This algorithm was disabled in the past due to the missing support in the Openswan IPsec implementation.

Restrains for FTP and Telnet

The maximum number of FTP or Telnet sessions can now be configured in the GUI. This measure was taken to prevent remote attackers to cause a denial of service (DoS) attacks to the router. Hirschmann recommends using secure protocols like SSH.

TLS Version Configuration

A minimal version of TLS protocol can now be configured in settings of HTTP in the GUI. TLS version 1.0, 1.1 or 1.2 can be chosen. It is recommended to use the last version of TLS. Support for other versions persists due to compatibility with various web browsers.

Report File Enhancement

A new section, called "Misaligned Access", is added to the report file. This section has the content of /proc/cpu/alignment file and will help us with potential debugging.

APN for PLMN 45435

The default APN for PLMN 45435 is changed to the "wbdata" string.

Fixed Issue with VLANs

We have fixed issues when creating VLAN with ID 1 or 2, which was found in the new kernel version. Originally the system has reserved these VLAN IDs for internal usage. Now for internal usage, VLAN IDs 4091 and 4092 are reserved and not usable anymore.

Fixed SIM Unlocking

We have fixed issues with SIM card unlocking and unblocking that does not work properly since firmware 6.1.7.

Fixed Flags for Bridged Interfaces

We have fixed the status command to show flags of the physical interface that is a part of the bridge.

Fixed Vulnerabilities:

This update eliminates the following vulnerabilities

- CVE-2019-5108 and CVE-2019-18282 in the Linux kernel.
- CVE-2020-8597 in the pppd package.
- CVE-2018-10811 and CVE-2018-5388 in the strongSwan software.
- CVE-2020-11810 by an update to OpenVPN version 2.4.9.

For more details about the release, see the webpage at
<https://openvpn.net/community-downloads/>.

- CVE-2016-1503, CVE-2016-1504, CVE-2019-11577, CVE-2019-11578, CVE-2019-11579 and CVE-2019-11766 by update of the dhcpd package to version 7.2.5.
- CVE-2019-14834 by an update to dnsmasq version 2.81.

For more details about the release, see the webpage at
<http://www.thekelleys.org.uk/dnsmasq/CHANGELOG>

Updated inetutils Package

We have updated the inetutils package, collection of common network programs, to version 1.9.4. This update has fixed the misaligned memory access in ftpd that degrades overall system performance.

Updated sudo Command

We have updated the sudo command to version 1.8.31. This update has fixed a few security vulnerabilities including CVE-2019-14287, CVE-2019-18684 and CVE-2019-18634. For more details about the release, see the webpage at <https://www.sudo.ws/stable.html>.

OWL LPWAN - Network Type Selection

The cellular module of the affected router searches by default for LTE Cat M1 and GPSS/EDGE networks only. We have updated the module configuration to enable searching for the LTE Cat NB1 networks too. Type of the cellular network to be searched for can be set up in the GUI to automatic selection, GPRS/EDGE, NB-IoT or LTE-M.

OWL 3G - Fixed Kernel Crash

We have fixed kernel crash triggered by downloading a file at high speed through the mobile connection.

Software version 06.2.03

Added SNMP Programs

The `snmpget` and `snmpset` programs, coming from the Net-SNMP package, are added. Program `snmpget` is an SNMP application that uses the SNMP GET request to query for information on a network entity. Program `snmpset` is an SNMP application that uses the SNMP SET request to set information on a network entity. For more information about these commands, see help in the console or at <http://www.net-snmp.org/>.

TACACS+ Authentication Support

A TACACS+ authentication protocol is added. For more information see <https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-13.html>.

Improved RADIUS/TACACS+ Authentication

Added taking over a server user during the RADIUS/TACACS+ authentication. A new user account is created when the RADIUS/TACACS authentication has passed and no corresponding local user account exists. A user account created this way cannot be used for authentication to the router without the RADIUS/TACACS server.

APN for AT&T and FirstNet

The default APN for the AT&T SIM cards was changed to the "broadband" string.
The default APN for the FirstNet SIM cards was changed to the "firstnet-broadband" string.

Updated Status Command

The dealing with units for the amount of transferred data reported by the status command was changed. By now, the units were rendered dynamically (in KB, MB, etc.) only. From now, the verbose (-v) option displays the units just in bytes, which allows getting the exact value.

Increased Pending TCP Connections

The maximal number of pending TCP connections in the HTTP server was increased. This update has fixed the bogus SYN flooding detection that was recognized in the new kernel version.

Improved IPsec Settings

A control mechanism to avoid an invalid IPsec configuration is implemented.
The GUI of the IPsec configuration form is updated to check the values of DPD Delay and DPD Timeout. A warning message pops up when the entered value of DPD Timeout is less than the value of DPD Delay.

Improvements and bugfixes WiFi

- Reworked WiFi Restarting

A wrongly configured WiFi AP blocked a well-configured WiFi STA. Now WiFi AP and WiFi STA can start independently.

- Fixed Stuck WiFi

The WiFi may sometimes stop working suddenly. Only the restart of the router will make it work again. The issue is fixed by correcting the usage of the wake-up interrupt, which was not triggered by a correct flag.

- **Memory Leaks in WiFi Driver**
A few memory leaks in the Laird WiFi driver are fixed that could happen in several scenarios.

Fix for PAM RADIUS Plugin

The resolving of the hostname in the PAM RADIUS plugin is disabled to eliminate a delay in case the DNS server is not responding.

Fix for FTP Server

We have disabled the reverse IP lookup made by the FTP server to eliminate a delay in case the DNS server is not responding.

Fixed Keepalived Malfunction

Several issues with VRRP are fixed, which can be observed since firmware version 6.2.1. These issues relate to the new implementation of Keepalived software.

Fixed Restoring of the Default Settings

The process of restoring the default settings invoked by pressing the RST button is fixed. This issue relates to a user module that changes the default settings of the router. It now works correctly, even if the RST button is held during the booting.

Fixed AT Command Response

The application crash that may occur when processing a very long AT command response is fixed.

Fixed Ethernet Status Detection

Fixed detection of link status in Ethernet driver which may cause the interface to fall down. This issue was recognized in the firmware version 6.2.1.

Fixed Memory Access

We have fixed issues noticed in very rare events when executing various programs. This issue was recognized in the firmware version 6.2.1

Fixed IPsec Routing

Fixed routing of packets over the IPsec tunnel. It did not work properly in case the remote subnet overlaps the local subnet and when the local subnet was not on the eth0 interface. This issue was recognized in the firmware version 6.1.9 when the Openswan implementation was replaced by strongSwan.

Fixed L2TP Establishing

We have fixed an issue establishing an L2TP connection. This issue could appear when a client establishes a connection with a significantly slower server side.

Fixed hostapd Program

This update has fixed CVE-2019-16275 in the hostapd program.

Updated curl Program

The curl program was updated to version 7.67.0.

Software version 06.2.01

Support of WLAN modules

Firmware version 06.2.01 is the first version to support WLAN modules on OWL 4G devices.

Support of WLAN Multi-role Mode

The role called multi-role is utilized for the WLAN module. This role allows the module to operate as an access point (AP) and station (STA) simultaneously.

Note: OWL 4G WLAN products do not support multichannel mode, so the AP and STA must operate on the same channel only.

Load Balancing

One of the most significant updates in this firmware release is the new feature of data load balancing. This feature can be used to improve the distribution of workloads across multiple interfaces. It can be configured on Backup Routes configuration page by enabling backup routes switching and selecting the mode to the Load Balancing. Next, you can set interface parameters to control the load balancing as required. For detailed information, see the configuration manual of your router.

PAM RADIUS Authentication

Added support for PAM (Pluggable Authentication Module) RADIUS authentication method for different types of access to the router. For detailed information, see the configuration manual of your router.

Certificate Uploading

Certificates having the PEM or PKCS#12 format can now be directly uploaded via the GUI. All certification entries in the GUI have a new button to browse and load a certificate stored in a file. This file is then processed and the required information is loaded to the configuration page automatically.

VRRP Enhancements

VRRP (Virtual Router Redundancy Protocol) was enhanced with the support of VRRP ver. 3. Besides, the second instance of VRRP can be configured and active simultaneously with the first one. This can be useful in case the connection check for both IPv4 and IPv6 is required.

Upgraded Kernel

The kernel was upgraded to version 4.14.138.

Upgraded tcpdump tool

Upgraded tcpdump tool to version 4.9.3.

Upgraded iptables program

Upgraded iptables to version 1.4.21

Upgraded OpenSSL library

Upgraded OpenSSL library to version 1.0.2t.

Upgraded glibc library

Upgraded glibc library to version 2.30.

OpenVPN program upgrade

Upgraded OpenVPN program to version 2.4.7

curl program upgrade

Upgraded curl program to version 7.65.3.

Upgrade iproute2 program

Upgraded iproute2 program to version 4.14.1.

Software version 06.1.09

Support of IPv6

IPv6 is supported by OWL LTE, OWL LTE M12 and OWL 4G devices.

Support of static routes

Added support for static routes configuration. There is a new configuration page Static Routes in the router's web configuration GUI. If IPv6 is supported by the router, two separate configuration pages for IPv4 and IPv6 are available.

For more information see the Configuration manual of the router.

Support for user accounts backup

Added support for user accounts backup and restoration. This functionality is available in the router's web configuration GUI under Backup Configuration and Restore Configuration menu

items. Backed up are all user accounts created in the router including the passwords (hashed).

Support of L2TP

Added support of Layer 2 Tunneling Protocol (L2TP) in Linux kernel.

IPsec enhancements

We have made the following enhancements to the IPsec implementation:

- support for Galois/Counter Mode (GCM),
- support for DH (Diffie Hellman) ECP Groups,
- support for XAUTH,
- support for PubKey,
- reauthentication for IKEv2 can now be disabled.

Clickjacking and XSS defence

Defence against Clickjacking and XSS attacks was implemented. Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms.

Important note: From now, it is not possible to use the router's web interface inside another frame on a user's web page.

Delay reboot until firmware update finishes

Replaced the reboot applet in BusyBox with our implementation in cbox. It will delay the reboot while the firmware update process is in progress.

Statistic match extension for iptables

Added support for statistic match extension to iptables. This extension matches packets based on some statistic condition and is often used for data load balancing. It supports two distinct modes settable with the `--mode` option, random and nth. Visit Linux manual pages for a detailed

description of this extension.

Thumb instruction set

Added support for Thumb instruction set. Thumb instructions are either 16 or 32 bits long. Instructions are stored half-word aligned. Some instructions use the least significant bit of the address to determine whether the code being branched to is Thumb code or ARM code.

Disabled renegotiation of SSL connection

Disabled client-initiated renegotiation of SSL connection to HTTPS server. The reason for this change is the defence against the Denial of service (DoS) attacks.

Cellular network registration issue

Fixed an issue when, under certain conditions, the cellular connection was established even if the operator's name was not configured.

Registration to an unavailable cellular network

Fixed an issue when, under certain conditions, the MS class on the Telit LE910 cellular module was switched to CC (GSM only). This issue caused that the router was switched to the GSM mode only and has persisted in this mode even if the restart was performed.

Fixed statistic for daylight saving time adjustment

Fixed incorrect Mobile WAN statistic processing. Statistic from the previous day was deleted after the daylight time adjustment (if the DST feature was enabled in NTP service configuration). Configuration issue on the cellular module

IPsec tunnel termination

Fixed IPsec tunnel termination. This issue could cause an interruption of communication through the IPsec tunnel.

OpenVPN issue

Fixed crashes of OpenVPN daemon.

DNS translation issue

Fixed DNS64 translation issue on interfaces without IPv6 address configured.

Added string match extension to iptables

Added string match extension to iptables. This extension allows matching a string anywhere in a packet's data payload.

Improved cookies security

The secure flag is now set when sending a new cookie to the web browser within an HTTPS response. This cookie can not be later used for an HTTP communication due to security reasons.

Improved text fields processing

All leading white space characters are removed from input text fields when processing the entered data. Implemented on LAN, WiFi, IPsec, OpenVPN and Scripts configuration pages.

Changed operator entry processing

If an operator was entered into the Operator field on the Mobile WAN configuration page, the router will not establish a connection to another operator anymore.

Upgraded tcpdump tool

Upgraded tcpdump tool to version 4.9.2.

Upgraded OpenSSH tool

Upgraded OpenSSH tool to version 8.0p1.

Upgraded OpenSSL library

Upgraded OpenSSL library to version 1.0.2r.

Upgraded glibc library

Upgraded glibc library to version 2.25.

OpenVPN program upgrade

Upgraded OpenVPN program to version 2.3.18

curl program upgrade

Upgraded curl program to version 7.64.1.

dnsmasq program upgrade

Upgraded dnsmasq program to version 2.80.

Upgraded BusyBox program

BusyBox program was upgraded to version 1.29.3.

Upgraded Net-SNMP program

Net-SNMP program was upgraded to version 5.8.

Software version 01.2.04 (2018-07-12)

From 2018-07-16 the OWL LTE M12 including the Telit LE910-EU V2 cellular module will be delivered with the new Telit Firmware revision 20.00.403 and the new OWL LTE M12 Firmware revision 1.2.04 (2018-07-12).

The new Telit Firmware fixes the corruption of the flash memory in the Telit chip. In the past, a corrupted flash memory led to a communication error of the OWL LTE M12 mobile interface which required, in some cases, the re-flash of the Telit chip.

The new OWL LTE M12 Firmware revision 1.2.04 (2018-07-12) has some driver adaptations to operate with the new Telit Firmware revision 20.00.403.

We recommend updating the Telit Firmware to revision 20.00.403.

On the OWL LTE M12 the following Firmware constellation has to exist to have a working mobile connection:

OWL LTE M12 Firmware revision	Telit Firmware revision
01.2.04 (2018-07-12) or higher	20.00.403

The upgrade of the Telit Firmware can be performed by the FOTA-manual user module, which is shipped together with OWL LTE M12 Firmware 01.2.04.

We recommend the following update procedure:

1. Connect to the OWL LTE M12 via Ethernet.
2. Update the OWL LTE M12 Firmware to 01.2.04 (2018-07-12)
3. Check the new OWL LTE M12 Firmware revision on the web interface page "Device Information". It has to be 01.2.04 (2018-07-12).
4. Update the cellular module Firmware to 20.00.403. For detailed information refer to the "User Manual FOTA (Firmware Over-The-Air) user module" chapter "Manual update".
5. Check the new Telit Firmware revision on the web interface page "Mobile WAN status". It has to be 20.00.403.
6. Check the mobile interface. It has to be up and connected.

Software version 01.2.03 (2018-02-19)

- The software version 01.2.03 (2018-02-19) is released for the OWL LTE M12 only. It includes stability improvements for SIP.
- The SIP Gateway User Module version 1.0.4 (2018-02-20) is a bug fix release for the OWL LTE M12. This User Module has to be used together with the OWL LTE M12 software version 01.2.03 (2018-02-19) for proper functionality.
- The Self Phone Number User Module version 1.0.1 (2017-09-25) is the first release for the OWL LTE M12.

Software version 01.2.02 (2017-07-12)

- The software version 01.2.02 (2017-07-12) is released for the OWL LTE M12 only.
- The SCEP Client User Module version 1.0.0 (2014-08-28) is the first release for the OWL LTE M12

Software version 01.2.01 (2017-01-06)

- The Software Version 01.2.01 (2017-01-06) is the first release for the OWL LTE M12.
- The GPS User Module version 1.3.4 (2017-03-28) is the first release for the OWL LTE M12. It supports the gpsd version 3.16.
- The SIP Gateway User Module version 1.0.0 (2016-09-01) is the first release for the OWL LTE M12.

Comments

Open the web interface of the OWL LTE M12. **If you connect the first time to your OWL LTE M12**, enter the default IP address 192.168.1.1/24 (on ETH0) in your web browser. The default user name is admin and the default password for the admin user is printed out on the router's label.

Prior to the Software update, back up the OWL LTE M12 configuration file with "Configuration" "Backup Configuration". After that step, load the new OWL LTE M12 operating system into your device with "Configuration" "Software".