Change log for Weidmüller Industrial Security Routers IE-SR-2/6GT series

List of firmware changes (new features and bug fixes) of Weidmüller Router models

List of affected Router variants:

Article name	Article number
IE-SR-2GT-LAN	1345270000
IE-SR-2GT-LAN-FN	1489940000
IE-SR-2GT-UMTS/3G	1345250000
IE-SR-2GT-LTE/4G-US	2535780000
IE-SR-2GT-LTE/4G-EU	2535930000
IE-SR-6GT-LAN	2535940000
IE-SR-6GT-LTE/4G-US	2535950000
IE-SR-6GT-LTE/4G-EU	2535960000
IE-SR-2GT-LAN-M	2535980000
IE-SR-2GT-LTE/4G-EU-M	2535970000

Important note when using the Weidmüller u-link Remote Access Service:

1. The u-link Remote Access Service is supported by firmware since version 3.0.2 Build number 72728 or later. If a Router shall be used for u-link additionally to an existing configuration please upgrade the firmware to the latest available version without a factory reset (by disabling the checkbox “Set factory defaults of the new firmware”).

2. If you will use any 6-Port Router model with u-link you need at least to update to version 3.2.1 Build 79368 or later.

3. The u-link Remote Access Service can be used with each Weidmüller router model except the variant IE-SR-GT-LAN-FN which does not support any VPN functions.

Version 3.2.3, Build number 87950 Release date: December 03, 2018

Feature updates:

- Added IPsec Fallback mode for 3G mobile Variants
- Added new server addresses for u-link WWH server

Bug Fixes:

- When updating the firmware with version 3.2.3 build 86546 a configured and activated u-link instance automatically was disabled. As result the u-link instance had to be re-activated manually after update by setting again checkbox “Enable u-link instance” in menu “VPN → u-link” of the web interface.
- Improved check method to recognize and identify an inserted SIM based on the received SIM ICCID.
- Fallback function from WAN to 4G did not work correctly if WAN port was configured with static IP address.
- Fixed scanning of available mobile networks

Version 3.2.2, Build number 86546 Release date: September 14, 2018

Feature updates:

- Added mechanism to upload 4G mobile modem firmware useable for a specific provider (e.g. for US models different modem firmware versions have been to be used dependent on the provider like Verizon or AT&T).
- Extended 4G status view about installed mobile modem firmware.

- Implementation of additional parameters for mobile settings: roaming, allowed & preferred networks, network modes, forcing a connection to a specific carrier via Mobile Country Code(MCC) & Mobile Network Code(MNC).
- Implementation of function “Network Scan” for evaluation of available mobile networks.
- Implementation of additional status symbol for mobile network signal quality.

Bug Fixes:
- Improved stability of 4G modem configuration.
- Fixed bug with timeout in SNMP mobile disconnect.
- Update “openssl” to version 1.0.2p (fix of security vulnerability CVE-2018-0732 & CVE-2018-0737).

Version 3.2.2, Build number 83558 Release date: July 16, 2018

Bug Fixes:
- Improved interoperability of mobile network connections (Problem when setting APN).
- Handle SIM cards with variable ICCID length.

Version 3.2.2, Build number 82950 Release date: June 28, 2018

Feature updates:
- Improved stability of mobile connections with low signal strength.
- Improved performance of menu Diagnostics → 4G. New mobile connection parameters added.
- New SMS Service features for control and information (SMS traps) implemented (Note: Only available for variants with an integrated 4G modem).
- Additional SNMP parameters for requesting LTE/4G status data implemented.

Bug Fixes:
- Update openssl to version 1.0.2o to fix security vulnerability CVE-2018-0739.
- Internal debug messages removed from Eventlog.
- Update of expired Demo Certificates included in the firmware.
- Restriction of Ethernet ARP announcements and ARP response packets on network interfaces with the matching IP address and subnet.

Version 3.2.1, Build number 79368 Release date: January 18, 2018

Bug Fix:
- In Menu “Packet Filter” of Web interface neither existing firewall rule sets could not edited nor new ones could be added due to a Java script error. Trying to add a new firewall rule set was resulting in displaying an empty window (no contents were displayed). This problem was introduced in previous version V3.2.0, Build 78720.

Version 3.0.0, Build number 78720 Release date: December 19, 2017

Feature updates:
- Improved SSL parameters for internal web server (SHA1 and 3DES disallowed, SHA256 or AES 128/256 required).
- Allow configuration of interfaces on which DNS relay service is running (by default DNS relay service is enabled on each network interface.
- Improved SSL parameters for internal web server (SHA1 and 3DES disallowed, SHA256 or AES 128/256 required).

Bug Fixes:
- Improvement of system stability by optimizing memory controller parameters.
- Fix of denial of service vulnerability and Pre-authentication remote crash/information disclosure for clients when using “http_proxy_passthrough” in OpenVPN (CVE-2017-7520).
- Fix of dnsmasq function (CVE-2017-13704).
- Fix of OpenSSL vulnerability by update to version 1.0.2l (CVE-2017-3736 and CVE-2017-3735).
- Fix of unreliable detection when inserting a cellular SIM card.
- Fix of memory leak which could lead to problems regarding a cellular-based (mobile) u-link VPN connection.

Version 3.1.2, Build number 77018 Release date: July 14, 2017

Feature update:

- Adaption of behaviour when restoring a backup configuration via USB stick (using backup file of type <name>.cf2).
  New procedure:
  1. Copy cf2-backup file to USB stick (FAT or FAT32) into directory named settings.
  2. Plug USB stick into the Router and power-up / reboot the device (Router automatically will load the cf2-file).
  3. Wait around 1 minute until the Router is ready again (PWR LED is lit constantly), having loaded the parameters of the configuration file.
  4. Un-plug USB stick from Router.

  How to check the result of the import procedure via USB stick:
  1. Plug USB stick into a PC and check directory settings which now should have a new sub directory with name same as the device serial number (e.g. AX1367406). This directory contains a log file named settings.log created by the Router at configuration upload.
  2. Open text file settings.log and check the status of the restoring process (e.g. containing message “Device configuration successfully updated”).

Note:
If you will use the same USB stick - containing a general template configuration file - for an initial setup of several Routers, then each Router will create during the restoring process its own sub directory AX.... (based on the unique serial number) below directory settings containing in the sub directory the Router specific text file settings.log.

Bug Fixes:

- u-link: DNS related problems fixed in terms of WWH-function when DNS settings have been changed.
- Counters for dropped/overrun packets of Ethernet Interfaces (LAN / WAN) now will be reset at system boot.
- Now short DNS names (<4 characters) to be used with DNS provider dyndns.org are allowed.
- Bug fix in terms of static configured link parameters of Ethernet ports (no Auto-Negotiation). No change of configured parameters after system boot (Elimination of fallback to 10Mbit/half after reboot when no link is available).
- Bug fix in terms of assignment of the default gateway via 3G. A setting could be get lost when opening IP configuration page and applying the settings.
- Several security updates.

Version 3.1.0, Build number 74521 Release date: December 05, 2016

New features:

- A saved configuration file (with extension .cf2) created from any Router model (IE-SR-2GT-LAN, IE-SR-2GT-LAN-FN or IE-SR-2GT-UMTS/3G) now can be load into any other Router model. All relevant parameters of the target Router will be imported. Not relevant parameters (eg. 3G configuration parameters when importing a backup file from a 3G-Router to a LAN/WAN-Router) will be ignored.
- Update of OpenSSL library to version 1.0.2j
- Improved calculation of CPU Load

Bug Fixes:

- Fix of behavior of the user interface when configuring the “Client monitoring” function sending an alarm via mail. This feature got disabled if the mail server address has been changed.
- When uploading a configuration file a new self signed certificate for the HTTPS server is generated. The host name used on this new self signed certificate was taken from the running configuration (false) and not from the uploaded configuration (correct). This problem was only relevant for configurations where the host name explicitly was configured. By default the host name is automatically generated from the device serial number. For such a default setting the problem did not arise.
- Regarding a configured fall back Internet connection (from WAN to 3G) always the WAN-Port related DNS server was used and not the DNS configuration of the active Internet connection (either WAN or 3G). In case of an activated fallback connection to 3G the DNS was not switched to the server obtained from the mobile network.
- Automatic synchronization of an inserted USB stick when the Router is rebooting. This avoids a possible file system corruption of the stick when loading a configuration file (cf2) from the stick.
- Improved restoring of configuration via USB stick (using backup file with extension <name>.cf2). After successful loading of the cf2-backup file from USB stick the file extension always has been renamed to *<name>.cf2.rej* even on successful loading. Now the cf2-backup file (on USB stick) will be renamed correctly to *<name>.cf2.ok*.

- The “Logoff” button in the web interface did not logout the user in some cases but simply returned to page “System state”.

Version 3.0.2, Build number 72728 Release date: May 09, 2016

New features:

- Added support for u-link Internet connection via Proxy server
- Improved diagnostic management (status messages) for u-link registration process

Bug Fixes:

- Fixed display error of OpenVPN state on page “System state”
- Improved SSL parameters of internal webserver

Version 3.0.1, Build number 72391 Release date: March 02, 2016

New features:

- Update openssl to version 1.0.2g

Bug Fixes:

- Improved stability of u-link/OpenVPN connections.
- Fixed internal timing issue which temporary could lead to 100% cpu load

Version 3.0.0, Build number 72188 Release date: January 18, 2016

New features:

- Implementation of new VPN-based functionality to use the Router with the Weidmüller u-link Remote Access Service. This feature can be configured in menu VPN → u-link.
- An IPsec connection now can be configured in aggressive mode (additional to existing main mode).
- For configuring an IPsec connection several new encryption parameters now explicitly can be set.
- The Packet Filter (Firewall settings) has now the ability to filter on the VPN UP (online) condition. Thus a filter rule matches if the VPN UP LED is on or off. The VPN UP signal can be activated via u-link, OpenVPN or IPsec.

Bug Fixes:

- IPsec connections did not always come back online after changes of time or date on a device. Additionally more detailed IPsec debug information was included on the IPsec status web page.
- The needed time for changing the operational mode (from IP Routing to Transparent Mode and vice versa) has been improved.
- Temporary UMTS/3G connection problems could lead to a complete shutdown of a permanent OpenVPN client connection.

Version 2.7.0, Build number 69965 Release date: June 01, 2015

New features:

- 1:1 Network mapping now can also be used on network interfaces if they are configured using dynamic address assignment (DHCP or OpenVPN).

Bug Fixes:

- IPsec connections did not always come back online after changes of time or date on a device. Additionally more detailed IPsec debug information was included on the IPsec status web page.
- Syslog server support on remote OpenVPN links did not work properly.

Version 2.6.3, Build number 68963 Release date: February 10, 2015

Bug Fixes:

- Optimizing function ‘NTP relay server’
- Problem to manually reboot with selection of the second firmware image was fixed.

Version 2.6.3, Build number 68843 Release date: January 26, 2015

Bug Fixes:

- IP-Forwarding from WAN to LAN interface sometimes did not work properly. This failure behaviour was introduced in Version 2.6.3 / Build number 68653.
- DynDNS service could not be configured outgoing to LAN interface (No problem when configuring DynDNS for WAN interface). This failure behaviour was introduced in Version 2.6.3 / Build number 68653.

Version 2.6.3, Build number 68653 Release date: December 08, 2014

New features:

- Implementation of a fall back mechanism when the Firmware is updated. Even if the power supply fails while updating process (Phase Flashing) is running an abort never will result in a broken device.
- Implementation of a "reboot timer" in menu System→Reboot. This feature is quite useful to remotely test new configurations which might lead to a connectivity loss (e.g. based on an unintended firewall configuration). If the reboot timer is activated the device automatically will reboot after the configured time and will come back with the last saved configuration. The reboot timer can be deactivated in menu System→Reboot (Cancel Reboot)
- The Router configuration (Backup file of type *.cf2) now can be loaded also by using an USB stick. The cf2-file has to be placed on a USB Stick in the directory "settings" or "settings/<serial number>". The stick has to be inserted and the device has to be rebooted. The device will load the settings at boot time.

Bug Fixes:

- Patched OpenVPN DoS Bug CVE-2014-810. This update is recommended for all setups running the Router as OpenVPN server with untrusted clients.
- Filter wizard Java Script error was fixed on insertion of predefined rule sets. Was broken since 2.6.0

Version 2.6.0, Build number 67659 Release date: July 07, 2014

New features:

- Automatic fallback mode to a 3G connection if a remote target device no longer is accessible via the WAN port. It is now possible to actively monitor a target IP address via ICMP over the Ethernet link. In case of failures the 3G uplink will be activated.
- 3G interface now can be used for static device routes

Bug Fixes:

- OpenSSL Update to version 0.9.8za (CVS-2014-0224). Update is recommend for all OpenVPNusers with an IE-SR-2GT-xxx OpenVPN counterpart at least on one side of two devices. Otherwise the connection is vulnerable to a Man-in-the-Middle attack due to a OpenSSL bug if both sides of a VPN connection have a vulnerable version of the OpenSSL library

Version 2.5.1, Build number 67460 Release date: June 02, 2014

Bug Fixes:

- German Umlauts were broken on the Permissions page since version 2.3.2
- NTP time synchronization and NTP server relay features have undergone a big cleanup. This includes a new NTP server state page in the web interface. Update is recommended for everyone using the NTP server relay or a highly accurate time synchronization.
- 1:1 NAT now allows an overlapping of local network IP addresses and 1:1 NAT mapping address spaces. Previously the web interface blocked this configuration.

Version 2.3.3, Build number 66690 Release date: January 24, 2014

New features:

- Firmware adapted to be used also for new model IE-SR-2GT-LAN-FN, means that this firmware version can be used for all Weidmüller Router models
    - IE-SR-2GT-LAN →LAN/WAN Router. General features: Routing, Firewall, NAT, VPN IPsec and OpenVPN
    - IE-SR-2GT-LAN-FN →LAN/WAN Router. General features: Routing, Firewall, NAT, No VPN
    - IE-SR-2GT-UMTS/3G →LAN/WAN Router plus additional 3G interface. General features: Routing, Firewall, NAT, VPN IPsec and OpenVPN
- The integrated HTTPS web server now is using a unique self signed certificate generated on factory defaults.
- Performance improvements for pure layer 2 filter without connection tracking.

- 1:1 NAT did not work as uplink network mapping or on local networks with communication across attached IP routers

Bug Fixes:
- Web access restrictions to the HTTP(S) server on the 3G interface did not have an effect.
- 3G connections on private APNs without DNS servers were not marked as CONNECTED because the DNS server was missing.

Version 2.3.2, Build number 65829 Release date: September 20, 2013

Bug Fixes:
- The Forwarding table (Port- and IP-Forwarding) had a wrong sorting for more than 10 entries.
- Under special conditions the DNS server of the 3G interface was used even if the corresponding checkbox was disabled.

Version 2.3.2, Build number 65490 Release date: August 02, 2013

Bug Fixes:
- Problem to show the Forwarding table correctly in Web interface page was solved (caused by a Java script error occured by using Microsoft Internet Explorer).
- A “Dial-On-Demand“ configured 3G/UMTS connection was unintentionally initiated each time a configured NTP time server tried to do a time synchronization even if internal IP addresses are used for NTP time server (cause by an unintended DNS lookup).
- The internal connection tracking table was increased to 32768 entries providing more robustness against DoS attacks and high load.

New features:
- Forwarding table (IP and Port forwardings) now has a new column for comments
- IPsec connections now can be switched by using the VPN key input. Configured connection entries have to be set to the mode “Active (Switched)”

Version 2.3.1, Build number 64408 Release date: April 12, 2013

Bug Fixes:
- Web configuration: Removed the possibility to disable the HTTP server completely in menu ‘Web server’. Use alternatively menu ‚Web access‘ to disable HTTP access.
- Web access control on the LAN port did not work. Access was allowed in any case.
- Function ‘Client monitoring’: Round trip time to control connected clients (if still alive) now can be set up to 5000 ms as maximum. Old maximum round trip time of 1000 ms was very noisy on 3G links.
- Explicit setting of Ethernet transmission mode like 100 MBit/half duplex was not applied on reboot after power down. Instead auto negotioation was used again.

New feature:
- Function ‘Client monitoring’: Allowing reset of the 3G modem if a client monitoring entry fails. This is very helpful on special M2M APNs which might need a 3G network re-registration after some time.

Version 2.3.0, Build number 63969 Release date: March 14, 2013

Bug Fixes:
- Fixed problem using IP aliases in Forwarding table.
- OpenVPN web interface: Now errors will be displayed if wrong options are entered.
- If a configured “Forwarding entry” was changed all running connected communication streams were not reclassified directly after the change (only after reboot).
- IE 8.0 Java Script error occurred if configuring a “Forwarding entry” by web interface.
- OpenVPN with NTLM Proxy Authentication contained a bug which could lead to not working proxy tunneling depending of the proxy vendor. This issues was described in “Public OpenVPN Ticket 172”. (https://community.openvpn.net/openvpn/ticket/172)
- “Save Only“ mode web interface improvements regarding Reboot and Save buttons.

New features:
- Implementation of new “Forwarding table” with below described features:
  - Optional setting of “Source NAT” for forwardings to hide the original source.
  - Conditional source matching to enable a forward only for special addresses.

- IP Forwarding with IP aliases on VPN channels like IPsec or OpenVPN to run additional virtual IPs on the VPN which will get forwarded to the local network.
- No more limitations on the number of forwards (before max. 11 forwardings)
- Configuration of Port- or IP-Forwardings independent of the IP configuration NAT interface (can now be used without having activated “NAT masquerading” either on LAN- or WAN-Port.

Version 2.2.9, Build number 63331 Release date: January 15, 2013

Bug Fixes:

- If a configured paket filter was changed, all running connected communication streams were not reclassified directly after the change (only after reboot).

Version 2.2.8, Build number 63139 Release date: December 19, 2012

Bug Fixes:

- PPPoE password edit with Firefox 15 was broken.
- Ping test on „save only“ mode was broken.
- The VPN LED did not work on other OpenVPN interfaces than VPN1.
- Modbus/TCP API calls for OpenVPN reworked. The OpenVPN connection must now be configured without permanent and Modbus/TCP will switch it on and off like a VPN Key event.

New features:

- Complete new OpenVPN web interface with many new features:
  - Implementation of OpenVPN user authentication and VPN-IP-Address assignment using a RADIUS server.
  - Optionally user authentication by User name / Password (additonally to certificate authentication).
  - OpenVPN server with per Client IP address and common name / user name mapping including per client OpenVPN internal routes - “iroutes”.
  - Any TCP/UDP port of OpenVPN-Server instances now can be used.
  - OpenVPN cipher can be configured.
  - Complete support for the OpenVPN “redirect-gateway” feature.

Version 2.2.7, Build number 62350 Release date: September 19, 2012

Bug Fixes:

- Running OpenVPN processes did not recognize changes of the DNS configuration.
- Firmware updates from older versions to version 2.2.7 using packet filter rules with stateful or automatic connection tracking will lead to a malfunctioning packet filter. The bug was introduced in version 2.2.7 Build 62062. This bug also effects NAT and port forwarding. The same problem can occur if a “settings file or “SIM card backup” with an older configuration gets loaded into version 2.2.7 Build 62062.
- Further improved 3G Link Stability

New features:

- Implementation of NTP server relay.
- Higher data throughput if the device runs without statefull filter rules.

Version 2.2.6, Build number 61875 Release date: August 13, 2012

Bug Fixes:

- Behavior of setting capacity-buffered realtime clock changed. At delivery time (before first boot of Router) the real time clock is set to production date of Router. If the Router is running more than 24 hours then each time when 24 hours have been passed, then the current date/time will be flashed into the memory as new initial date/time if the Router will be shutdown and powered on again.

New features:

- Implementation of uploading PEM certificate files of type “.crt”.

Version 2.2.5, Build number 61501 Release date: June 13, 2012

Bug Fixes:

- SCEP can now be used with automatic renewing and challenge password in combination.

Version 2.2.4, Build number 61357 Release date: May 23, 2012

Bug Fixes:

- OpenVPN HTTP proxy field was restricted to 15 characters, this has been fixed.
- NAT and port forwarding on L3VPN OpenVPN network devices did not work properly.

New features:

- The port forwarding is now called forwarding and was extended to forward on an IP/IP base too using IP aliases on the public interface.
- The VPN LED can now be configured to either run on one of the OpenVPN connections or on Ipsec.

Version 2.2.3, Build number 61087Release date: April 27, 2012

Bug Fixes:

- Upload of certificate files of type ".pem", was broken in version 2.2.3 Build 61052.
- 3G interface bug fixes on DNS server & SIM card state.

New features:

- The OpenVPN integration now supports the configuration of the OpenVPN parameters lzo, tun/tap device types and UDP.
- 3G web interface GUI is now easier to use.
- Ethernet Link Mode can be configured manually.