HIRSCHMANN
A BELDEN BRAND

List of Issues HiSecOS

ID	Since Release	Fix Release	Date	Description	Workaround	Correction
1	01.0.00	---	8/16/2012	If Proxy ARP is enabled on the router interface Proxy ARPs may be answered on the same interface as they originated.	-	Necessary behavior for certain NAT use cases, no change planned.
2	01.0.00	---	10/18/2012	The standalone web interface just accepts changes in the preferences after a restart.	Restart the standalone web interface. Option to download a standalone web interface was removed in version 01.2, HiView is the preferred method to access the GUI.	No change planned.
3	01.0.00	01.1.00	8/22/2012	Audit Trail does not log all configuration changes made in the web interface.	-	Fixed in 01.1.00.
4	01.0.00	---	4/18/2012	The link status does not switch to the correct speed when a mismatch occurs. For example, if a port is manually set to 10 Mbit/s and the peer is set to 100 Mbit/s.	Use autonegotiation or configure the port speed properly.	Hardware related limitation.
5	01.0.00	---	8/1/2012	Saving a large configuration to the device can take several minutes.	-	Optimization planned for future release.
6	01.0.00	01.1.00	4/20/2012	The routing mode supports a maximum of 500 pkt/sec of 64byte length.	-	Fixed in 01.1.00.
7	01.0.00	01.1.00	11/15/2012	During a configuration save a device reboot can be started (e.g. via a different interface web/cli/mib). This results in a damaged configuration and therefore the device will restart with default settings.	After saving the configuration please wait 5 seconds before initiating a reboot.	Fixed in 01.1.00.
8	01.0.00	02.0.00	10/16/2012	For NAT rules no logs and traps are generated.	-	Fixed in 02.0.00.
9	---	02.0.01	11/14/2014	In rare situations, a reboot might occur in case of high memory load.	-	Fixed in 02.0.01.
10	01.0.00	No fix	2/5/2015	If the Java security settings are set to very high, the HTTPS connection cannot be established to a device as long as the default certificate is used.	Exchange the web server certificate on the device with one that contains an OSCP and/or CRL URL (preferred). Alternatively, weaker Java security settings can be used.	No fix planned.
11	01.0.00	03.0.01	10/1/2015	Using a sysName that is not a valid hostname or fully qualified domain name (FQDN) can lead to incorrect log entries when using a remote syslog server for logging.	Ensure that the sysName is a valid hostname or FQDN.	Fixed in 03.0.01.
12	03.0.00	04.0.00	10/16/2015	Setting the ping tracker timeout to a value greater than the ping interval causes the tracker state to remain in one state. The state depends on the user specified relation between the lost ping replies and the received ping replies.	Set the ping timeout to a value lower than the ping interval.	Fix planned for a next release.
13	03.0.00	03.0.02	2/5/2016	If VRRP is configured on an interface, then the device does not apply packet filtering rules to traffic passing through the VRRP interface. However, the rules are applied to traffic passing through the underlying routing interface and the global policy still applies. For example, if the global policy is set to 'drop' or 'reject', then this results in traffic passing the VRRP interface being dropped or rejected, respectively. If the policy is set to 'accept', then the packets pass through the VRRP interface unfiltered.	-	Fixed in 03.0.02.
14	02.0.00	03.0.02	2/20/2017	In a 1:1 NAT setup, if one of the two involved ports temporarily loses its link, then NAT may stop forwarding packets.	-	Fixed in 03.0.00.
15	03.0.00	03.0.02	7/1/2015	HTTP(S) does not limit the rate or number of login attempts, which allows an unauthorized user to guess a large number of passwords in a short time.	Limit HTTP(S) access to trusted IP addresses.	Fixed in 03.0.02.
16	03.0.01	03.0.02	10/26/2016	The device sporadically does not recognize an SFP when inserting it or booting the device.	Reinsert the affected SFP or reboot the device. If the problem persists, then repeat this step.	Fixed in 03.0.02.
17	02.0.00	---	11/14/2017	If a VPN has a connection passphrase set for the private key, the device decrypts the private key even if it has already been uploaded to the device in cleartext. As a result, a connection with this passphrase and a cleartext private key will not be established.	If you use cleartext private keys, remove the connection passphrase.	Improvement planned for a future release.
18	02.0.00	---	11/15/2017	The certificate upload in the VPN wizard does not work.	Upload the certificate(s) in the corresponding dialog before starting the wizard.	Fix planned for a next release.
19	02.0.00	---	7/7/2017	The device drops the packets for which it does not have a matching route. This includes packets that are intended to pass through an IPsec connection.	Add a route for the subnets attached to the remote endpoint of the VPN connection. This can also be a default route. Such a route lets the packets pass the routing stage into the IPsec subsystem.	No fix planned.
20	03.1.00	03.1.01	1/31/2018	The device might stop sending proxy ARP responses. This prevents the 1:1 NAT and Double NAT types from working correctly.	Enter static ARP entries in the end devices for the NAT'ed IP address(es) with the MAC address of the corresponding interface of the EAGLE.	Fixed in 03.1.01.
21	03.1.00	03.1.01	2/8/2018	The device might send a CHILD_CREATE_SA messages without any proposal, which can cause other IPsec implementations to behave incorrectly.	-	Fixed in 03.1.01.
22	03.1.00	03.1.01	2/14/2018	During device startup, NAT rules stored in the configuration are applied before the interfaces are fully configured. As a result, the NAT rules become inactive.	Manually enable the disabled rules after the device has started up.	Fixed in 03.1.01.
23	03.1.01	03.2.00	9/28/2018	Using "any" as a remote gateway in VPN "Endpoint and Traffic Selectors" functionality will lead the device to reboot.	Configure an IP address for the remote gateway instead of "any".	Fixed in 03.2.00.
24	03.2.00	03.2.01	9/5/2018	The CLI command "clear ip udp-helper" does not clear the configuration.	Instead use "ip udp-helper server delete dhcp <a.b.c.d>" to delete entries one by one.	Fix planned for 03.2.01.
25	01.0.00	03.1.02	9/7/2018	In rare situations an received invalid truncated TCP paket can bring the device into an unstable state were it's stops to process pakets.	-	Fixed in 03.1.02.
26	02.0.00	03.0.01	11/5/2015	Both VRRP routers become Master if using RMA	-	Solution: add a rule to always accept vrrp packets
27	03.4.00	---	2/6/2020	After reboot via HTML web GUI, system gives login prompt immediately but can't login via same session without refresh.	After reboot via Web, wait for couple of minutes and refresh the web page before entering login credential.	To be fixed in future release.