List of Issues EAGLE20, EAGLE One

ID	Since Release	Fix Release	Date	Description	Workaround	Correction
1	04.3.00 NG		6/23/2008	The device does not support the forwarding of GVRP frames.		No fix planned.
2	04.3.00 NG		7/3/2008	A VPN connection between the Eagle software version up to 04.2.0x and the Eagle software version from 04.3.00 can be established only if the IPSec lifetime is less than or equal to the IKE lifetime on both devices. Additionally the configuration has to be the same on both devices.	See description.	No fix planned.
3	04.3.00 NG		7/16/2008	VPN connections are supported on the external interface only.		No fix planned.
4	04.3.00 NG		7/18/2008	If a packet filter rule for IP filtering is added with "reject", the handling of rejecting TCP frames is different dependent on the protocol configured ("TCP" or "any").		No fix planned.
5	04.3.00 NG		8/27/2008	The ACA11 is not supported.	Use ACA21	No support planned.
6	04.3.00 NG	04.4.00	9/18/2008	Using Microsoft (R) Windows Vista (TM) a user can not save file on the local computer using the Web Interface.	Execute Internet Explorer as Administrator and saving of files is possible.	Added note to the manual in 04.4.00.
7	04.3.00 NG		9/25/2008	The DHCP server can assign IP addresses in transparent mode to the internal interface only. The firewall must not be closed for DHCP Server traffic (UDP frames with destination port 67 and source port 68).		No fix planned.
8	04.3.00 NG		9/26/2008	SNMP traps with destination IP address on the external interface are sent in Router/PPPoE mode with the IP address of the internal interface.		No fix planned.
9	04.3.01	04.4.00	2/16/2009	FTP clients, which are using active FTP in combination with NAT are blocked in some cases by the Firewall.	Use passive FTP.	Fixed in Release 04.4.00.
10	04.3.00 NG	04.3.02	3/25/2009	Using Internet Explorer 8 or Firefox 3.0.8 and Java 6 Update 13 the Eagle web applet can not be started.		Fixed in Release 04.3.02.
11	04.3.00 NG	04.3.02	4/14/2009	System crash with migrated configuration from Eagle mGuard with VPN connection having PSKs larger than 32 characters.		Fixed in Release 04.3.02.
12	04.3.00 NG	04.3.02	5/12/2009	The user firewall sends authentication requests every 60 seconds while the login screen is open when using radius server.		Fixed in Release 04.3.02.
13	04.3.00 NG	04.4.00	6/15/2009	The manual and the web interface help describe the packet filter port range configuration wrong: <> inside >< outside The correct configuration syntax for port ranges has to be: >< inside <> outside The start and end ports do not form part of the port range.		Manual changed in Release 04.4.00.
14	04.3.00 NG	04.4.00	6/16/2009	VPN connections can have PSKs with 32 characters maximum.		Fixed in Release 04.4.00.
15	04.3.00 NG	04.4.00	6/16/2009	Clicking the "Write" button in the VPN dialog causes the remote control password to be overwritten.	Re-enter the remote control password each time before clicking the "Write" button.	Fixed in Release 04.4.00.
16	04.3.00 NG		9/25/2009	Note: The systen name can have a length of 63 characters.		No fix planned.
17	04.4.00	05.0.00	12/10/2009	The Packetfilter Dialogs have a inconsitened behaviour. Under some circumstances not all changed rows are written to the device.	Press the "Write" button after you finned editing a row or use the offline configuration utility.	Fixed in Release 05.0.00.
18	04.3.00 NG	05.0.00	12/10/2009	Under rare circumstances a temperature trap is sent although the limits are not exceeded.	Compare the temperature value contained in the Trap with the threshold values.	Fixed in Release 05.0.00.
19	04.4.00	05.0.00	12/10/2009	VPN connection using the aggressive mode may not respond to Dead Peer Detection (DPD) packets.	Deactivate DPD on the remote peer.	Fixed in Release 05.0.00.
20	04.3.00 NG	05.0.00	1/12/2010	The user firewall uses for the firewall entry always the IP address of the PC on which the user logged in, thus as source address in the user firewall rule only %authorized_ip is possible.		Fixed in Release 05.0.00.
21	04.3.00 NG		9/6/2010	Please keep in mind, that a VPN connection (IKEv1 and IKEv2) can be interrupted for a short time after the expiration of the lifetime.		No fix planned.
22	04.3.00 NG		9/27/2010	Hardware errors (e.g. CRC errors) can not be counted in the port statistics error counter (ifError).		No fix planned.
23	04.3.00 NG		10/13/2010	The information for NAT-T in IPSec tunnel (encapsulation) is displayed wrong for IKEv2 connection.		No fix planned.
24	04.3.00 NG	05.0.00	10/29/2010	If the login window of the user firewall is closed, an active logout of the user is not longer possible.	After expiration of the defined time-out the user will be automatically logged out.	Fixed in Release 05.0.00.
25	04.3.00 NG	05.1.00	7/2/2010	additional note: the DHCP server can lease at most 1024 IP addresses.		Has been added to the manual.
26	05.0.00	05.1.00	10/29/2010	The default values for the NTP server in the manual are wrong: The correct values are: "Server request interval" 64 s. "Anycast send interval" 128 s.		Corrected in the manual for Release 05.1.00.
27	05.0.00	05.1.00	11/4/2010	additional notes: CLI The clear config command does not clear the name of the active configuration profile. The command "save profile " shall be used to store the cleared configuration under a new name! Transparent redundancy -> Firewall State Table Synchronization (Communication state): Not receiving packets from the others side is an indication, that something is wrong, but the real Layer 2 redundancy state can only be checked on the switches! It also can happen, that if nothing has to be exchanged in the ft sync protocol, there is no communication, but everything is alright!		Has been added to the manual.
28	05.0.00	05.1.00	11/8/2010	additional note: In PPPoE mode not all PPPoE packets are counted in the external interface counter statistics.		Added to the manual for Release 05.1.00.
29	04.3.00 NG	05.1.00	12/7/2010	To handle all redundancy failure scenarios correctly, you should configure ICMP host check target in the internal and external network.		Shall be added to the manual.
30			4/4/2011	Remote VPN activation/deactivation with a URL containing the user and password as described in the manual does not work with some versions of the Internet Explorer: "https://vpn:test123@10.10.10.3/nph-vpn.cgi?name=connection&cmd=up"	Using instead the URL "https://10.10.10.3/nph-vpn.cgi?name=connection&cmd=up" and a following password dialog box works also with Internet Explorer.	
31	05.0.00	05.1.00	5/23/2011	IKEv2 together with Hirschmann Address Mapping (HAM) is not working in Version 05.0.00.	Use IKEv1 together with HAM.	Fixed in Release 05.1.00.
32	04.4.00	05.1.00	3/16/2011	When a combination of 1:1 NAT is used together with Router redundancy under rare circumstances where a redundancy switch over takes place, the EAGLE responds to an ARP request with its physical MAC address instead of the virtual MAC address.	-	Fixed in Release 05.1.00.
33	04.3.00 NG	05.1.00	5/31/2011	Static route entries with 32 bits network mask (host entries) are not forwarding the traffic to the configured gateway.	Use a network mask less than 32 bits.	Fixed in Release 05.1.00.
34	05.0.00	05.2.00	6/20/2011	The device itself becomes unreachable when the forwarding of IP fragments is disabled in Transparent Mode.	Do not disable forwarding of IP fragments in Transparent Mode.	Fixed in Release 05.2.00.
35	04.3.00 NG		10/26/2011	The firewall does not accept ARP responses in 802.3 frame format (with LLC/SNAP header). It only accepts ethernet II frame ARP responses to its ethernet II frame requests.	Configure your devices to use the ethernet II frame format.	Routing and device management access using 802.3 frames is a not supported feature.

List of Issues EAGLE20, EAGLE One

ID	Since Release	Fix Release	Date	Description	Workaround	Correction
36	04.3.00 NG	05.2.00	2/23/2012	If the SSH connection is closed while the CLI has buffered output (output which is stopped at a page break with "more"), the system will no longer be reachable.	Quit buffered output before leaving SSH connection or use the command "set numlines 0" to avoid buffered output.	Fixed in Release 05.2.00.
37			1/13/2012	The VPN connection might be established even if the configuration on both sides of the VPN is different regarding the tunnel and transport mode, e.g. tunnel mode initiator and transport mode responder.	Check configuration on both sides of the tunnel.	-
38	04.3.00 NG		3/21/2012	The NAT functionality (1:1 NAT, IP Masqerading, Port Forwarding) does not support VLAN tagged interfaces, i.e. if you have enabled VLAN tagging, it is not possible to use the NAT functionality.	-	Not planned.
39	05.0.00		8/27/2012	Fragments are blocked by the IP packet-filter header checks if the don't fragment bit is set together with the fragment bit in the IP header.	Please disable packet-filter IP header checks.	No change planned.
40	04.3.00 NG		8/24/2012	If an invalid web server certificate is uploaded, it might be that the java applet does not accept the web server certificate, although the web server accepts it. In this case the web interface will not work.	Clear the web server certificate in the CLI.	No fix planned.
41	04.3.00 NG	05.2.01	7/4/2012	A user firewall user (when authenticated against RADIUS server) is able to login to the EAGLE20 web interface with read-only access.	-	From version 05.2.01 different service types in RADIUS configuration are used for user firewall users and system login users.
42	04.3.00 NG	05.3.03	7/5/2016	If radius authentication is configured, then passwords longer than 128 characters cause the device to reboot.	-	Fixed in 05.3.03
43	05.3.00	05.3.03	7/11/2016	The internal clock drifts more than the 500ppm allowed by NTP.	-	Fixed in 05.3.03
44	04.3.00 NG	05.3.03	7/26/2016	The device does not recognize a new ACA-21.	Connect the ACA-21 to a PC USB port and mount its file system.	Fixed in 05.3.03. The first time a new ACA-21 is plugged into the device, mounting may be delayed up to one minute. To avoid this delay, perform the workaround.
45	05.3.00	05.3.04	10/4/2016	If you change the signal contact from its default (show the device status), the status LED incorrectly signals a correct status with an off state.	-	Fixed in 05.3.04.
46	05.3.00	05.3.04	8/29/2016	If the device uses a multimode fiber connection, it may stop sending LLDP frames.	-	Fixed in 05.3.04.
47	05.3.00	05.3.05	2/13/2019	Internal clock drifts more than 2 minutes per day.	-	Fixed in 05.3.05.
48	04.3.00 NG	05.3.05	2/13/2019	ACA 21 and ACA 22 show wrong serial numbers.	-	Fixed in 05.3.05
49	04.3.00 NG	05.3.05	9/7/2017	Successive authentication list methods are processed even if previous method returned a reject.	-	Fixed in 05.3.05
50	04.3.00 NG	05.3.05	2/12/2018	Firewall is not forwarding EAPoL frames for 802.1X.	-	Fixed in 05.3.05 By default EAPOL messages will not be forwarded. In order to enable this please use the CLI command <packet-forwarding eapol enable> or use the Web GUI (Advanced -> Packet Forwarding -> EAPOL Checkbox).
51		05.4.01	1/7/2021	OpenSSL vulnerability (CVE-2020-1971)	-	Fixed in Release 05.4.01
52		05.4.01	11/11/2016	ntpd vulnerability (CVE-2016-4954)	-	Fixed in Release 05.4.01
53		05.4.01	11/11/2016	ntpd vulnerability (CVE-2016-4953)	-	Fixed in Release 05.4.01
54		05.4.01	3/6/2019	OpenSSL vulnerability (CVE-2019-1559)	-	Fixed in Release 05.4.01
55		05.4.01	3/7/2019	OpenSSL vulnerability (CVE-2018-0732)	-	Fixed in Release 05.4.01
56		05.4.01	3/7/2019	ntpd vulnerability (CVE-2016-9042)	-	Fixed in Release 05.4.01
57		05.4.01	10/21/2019	Several OpenSSL vulnerability (CVE-2019-1547, CVE-2019-1549, CVE-2019-1563)	-	Fixed in Release 05.4.01
58		05.4.01	5/29/2018	ntpd vulnerability (CVE-2018-0739)	-	Fixed in Release 05.4.01
59		05.4.01	10/5/2020	OpenSSL vulnerability (CVE-2020-1968)	-	Fixed in Release 05.4.01
60		05.4.01	5/3/2021	Several OpenSSL vulnerabilities (CVE-2021-3449, CVE-2021-23840, CVE-2021-23841)	-	Fixed in Release 05.4.01
61	05.4.01	05.4.02	12/20/2021	Web interface of eagleOne with firmware version 05.4.01 is not opening in HiView	-	Fixed in Release 05.4.02
62	05.4.01	05.4.02	4/22/2022	Device reboot observed when accessing the web interface from a PC with old JAVA version.	-	Partially fixed in Release 05.4.02 (crash re-observed on SDV) Final fix in Release 05.4.03
63			4/7/2022	Failed to load PKCS12 certificate for IPsec VPN tunnel.	Use PSK for IPsec VPN tunnel.	To be fixed in future release.
64			7/5/2021	out-of-sync messages in HiVision right after device startup.	-	To be fixed in future release.
65	05.4.02	05.4.03	6/9/2022	Crash observed on SDV devices for TLS1.1 and below.	-	Fixed in Release 05.4.03 (tested with JAVA7, JAVA8 using TLS1.2)