



ID	Since	Fixed in	Date	Variant	Description	Workaround	Correction
1	01.0.00		2012-08-16	EAGLE20/30	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		2012-10-18	EAGLE20/30	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	2012-08-22	EAGLE20/30	Audit Trail does not log all configuration changes made in the web interface.	-	Fixed in 01.1.00.
4	01.0.00		2012-04-18	EAGLE20/30	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		2012-08-01	EAGLE20/30	Saving a large configuration to the device can take several minutes.	-	Optimization planned for future release.
6	01.0.00	01.1.00	2012-04-20	EAGLE20/30	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	2012-11-15	EAGLE20/30	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	2012-10-16	EAGLE20/30	For NAT rules no logs and traps are generated.	-	Fixed in 02.0.00.
9		02.0.01	2014-11-14	EAGLE20/30	In rare situations, a reboot might occur in case of high memory load.	-	Fixed in 02.0.01.
10	01.0.00	No fix	2015-02-05	EAGLE20/30	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	2015-10-01	EAGLE20/30	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	2015-10-16	EAGLE20/30	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.	To be fixed in future release.
13	03.0.00	03.0.02	2016-02-05	EAGLE20/30	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	2017-02-20	EAGLE20/30	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	2015-07-01	EAGLE20/30	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	2016-10-26	EAGLE20/30	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		2017-11-14	EAGLE20/30	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	05.2.00	2017-11-15	EAGLE20/30	The certificate upload in the VPN wizard does not work.	Upload the certificate(s) in the corresponding dialog before starting the wizard.	To be fixed in future release.
19	02.0.00		2017-07-07	EAGLE20/30	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	2018-01-31	EAGLE20/30	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 NATed 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	2018-02-08	EAGLE20/30	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	2018-02-14	EAGLE20/30	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	2018-09-28	EAGLE20/30	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	2018-09-05	EAGLE20/30	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.	Fixed in release 03.2.01.
25	01.0.00	03.1.02	2018-09-07	EAGLE20/30	In rare situations an received invalid truncated TCP packet can bring the device into an unstable state were it's stops to process packets.	-	Fixed in 03.1.02.
26	02.0.00	03.0.01	2015-11-05	EAGLE20/30	Both VRRP routers become Master if using RMA	-	Solution: add a rule to always accept vrrp packets
27	03.4.00	03.5.00	2020-02-06	EAGLE20/30 EAGLE40-03	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.
28	03.4.00		2020-01-15	EAGLE40-03 EAGLE40-07	L4 protection is not working for the services not running on DUT.	In current software, L4 protection works fine for all the services running on Eagle device.	To be fixed in future release.
29	03.4.00		2020-02-06	EAGLE40-03 EAGLE40-07	Land attack filter is not working for virtual interface.	In current software, Land attack filter works fine for physical interface.	To be fixed in future release.
30	03.3.00	04.0.00	2019-11-20	EAGLE40-03 EAGLE40-07	SFP details are not getting displayed via cli "show sfp", though data transfer is successful.	-	Fixed in release 04.0.00
31	03.4.00	03.4.01	2020-03-26	EAGLE20/30	Temperature measurement not working	-	Fixed in 03.4.01
32	03.3.00	03.4.01	2020-02-19	EAGLE20/30	VRRP SFP interface stuck in init state after changing the VRRP config and performing save and reboot	-	Fixed in 03.4.01
33	03.5.00	04.3.00	2022-02-14	EAGLE20/30 EAGLE40-03 EAGLE40-07	http (CVE-2021-22819)	-	Fixed in Release 4.3.00
34	04.1.01	04.2.00	2021-07-28	EAGLE40-07	EAGLE reboots during ARP cache saturation storm.	-	Fixed in release 04.2.00



ID	Since	Fixed in	Date	Variant	Description	Workaround	Correction
35	03.5.00	04.2.01	2018-04-26	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2018-7184)	-	Fixed in release 04.2.01
36	01.0.00	04.1.00	2019-06-19	EAGLE20/30 EAGLE40-03 EAGLE40-07	An integer overflow flaw was found in the way the Linux kernel's networking subsystem processed TCP Selective Acknowledgment (SACK) segments. A remote attacker could use this flaw to crash the Linux kernel by sending a crafted sequence of SACK segments on a TCP connection with small value of TCP MSS, resulting in a denial of service (DoS)	-	Fixed in release 04.1.00
37	HiSecOS-03.2.00	04.2.00	2021-03-31	EAGLE20/30 EAGLE40-03 EAGLE40-07	OPC DPI forwards any packet that has less than 20 bytes of TCP payload.	-	Fixed in release 04.2.00
38	03.2.00	04.2.00	2021-03-31	EAGLE20/30 EAGLE40-03 EAGLE40-07	OPC Classic Enforce Denial of Service attack	-	Fixed in release 04.2.00
39	4.3.00	04.3.01	2022-04-06	EAGLE20/30 EAGLE40-03 EAGLE40-07	Memory leak observed in Eagle after long durations of snmp requests	-	Fixed in release 04.3.01
40	03.5.00		2020-10-21	EAGLE20/30 EAGLE40-03 EAGLE40-07	Eagle web becomes unresponsive, once web remain open for more than a day with idle timeout set as value 0. Common issue in HiOS and HiSecOS HTML web.	If idle timeout is set to default or any value other than 0, this issue won't appear.	To be fixed in future release.
41	03.2.00	04.2.00	2019-04-26	EAGLE20/30 EAGLE40-03 EAGLE40-07	Invalid/Special character are allowed in VLAN name	-	Fixed in release 04.2.00
42	HiSecOS-04.0.00	04.1.01	2021-06-02	EAGLE40-03 EAGLE40-07	Multiple ports provided in L2 filter rule under src-port or dst-port, were not getting applied in iptables.	NA	Fixed in release 04.1.01
43	03.5.00	4.2.01	2019-03-07	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2016-9042)	-	Fixed in release 04.2.01
44	03.5.00	04.0.00	2020-08-20	EAGLE40-03	Downgrade from 03.5.00 to 03.4.01 release is not possible via sftp/Web/ACA.	-	Fixed in release 04.0.00
45	04.0.00		2020-11-26	EAGLE40-03 EAGLE40-07	Upto 999 L2 filter rules can be created in Eagle 40 device.	As per current information, none of the customer is using rules even close to 999.	To be fixed in future maintenance release.
46	04.1.01	04.3.00	2021-09-16	EAGLE40-03 EAGLE40-07	Devices attached via VLAN router interfaces are not reachable via VPN	VPN tunnel works fine on VLAN interface, it is just end device added on VLAN interface are not reachable via VPN tunnel.	Fixed in release 04.3.00
47	04.3.00		2022-03-07	EAGLE40-03 EAGLE40-07	When user switches from L3 DPI to L2 DPI on same physical interfaces, Device Reboot required in order to pass traffic.	This behavior only surfaces when the same interface which were previously part of routing DPI are changed to transparent DPI & Post reboot traffic resumes.	To be fixed in future release.
48	03.5.00	04.2.01	2021-08-16	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2020-15025)	-	Fixed in release 04.2.01
49	04.1.01	04.2.00	2021-07-14	EAGLE40-03 EAGLE40-07	VRRP long recovery time after reboot of the master	-	Fixed in release 04.2.00
50	04.3.00		2022-03-10	EAGLE40-03 EAGLE40-07	When user modify packetfilter rule from enforcer to Accept, profile index not resets to zero. Which causes drop in traffic.	Profile index can be reset to zero via CLI or rule can be delete and reconfigure with appropriate configuration.	To be fixed in future release.
51	03.5.00	04.2.00	2020-07-22	EAGLE40-03 EAGLE40-07	No support of copper SFP in device, it might work with hot plug in and port goes down after reboot.	-	Fixed in release 04.2.00
52	01.0.00	04.1.00	2018-11-15	EAGLE20/30	Net-SNMP vulnerability (CVE-2018-18065)	-	Fixed in Release 04.1.00
53	04.0.00	04.2.01	2020-12-04	EAGLE40-03 EAGLE40-07	Vlan tagged packet not getting filtered by I2 filtering if matched on vlan interface with untagged egress port.	-	Fixed in release 04.2.01
54	04.1.00	04.3.00	2020-07-23	EAGLE20/30 EAGLE40-03 EAGLE40-07	net-snmp (CVE-2019-20892)	-	Fixed in Release 4.3.00
55	03.5.00	04.3.00	2020-01-03	EAGLE40-03 EAGLE40-07	OpenSSL (CVE-2019-1551)	-	Fixed in Release 4.3.00
56	03.4.00	03.5.00	2020-05-26	EAGLE20/30	IPV4 ACL configuration via web interface returns error.	Issue has been fixed in latest software.	Fixed in 03.5.00 Release.
57	04.2.00	04.2.01	2021-11-29	EAGLE40-03 EAGLE40-07	OPC valid packet is getting dropped in running DPI process in Eagle40	-	Fixed in release 04.2.01
58	03.5.00	04.2.01	2021-08-24	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2020-13817)	-	Fixed in release 04.2.01
59	03.5.00	04.2.01	2021-08-24	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2020-11868)	-	Fixed in release 04.2.01
60	04.0.00	04.0.01	2020-12-08	EAGLE40-03 EAGLE40-07	Eagle40 release 04.0.00 throughput improvement is needed, as it is lower than the previous release.	No functionality impact.	Fixed in release 04.0.01
61	03.5.00		2020-07-29	EAGLE40-03	Few Eagle40-07 hardware get reboot, once we press button labeled as "RESET" on device.	In current version of software, this button has no functionality implemented, hence usage is not recommended.	Other hardware with correct jumper settings does not get reboot, once we push RESET button.
62	04.1.00	04.2.01	2021-08-26	EAGLE20/30 EAGLE40-03 EAGLE40-07	OpenSSL vulnerabilities (CVE-2021-3712, CVE-2021-3711)	-	Fixed in release 04.2.01
63	03.4.00	04.2.01	2019-09-16	EAGLE20/30 EAGLE40-03 EAGLE40-07	U-boot vulnerability (CVE-2019-13103)	-	Fixed in release 04.2.01
64	HiSecOS-03.5.00	04.1.01	2021-04-29	EAGLE40-03 EAGLE40-07	Vlan-1 can't be used as routing interface in Eagle40 device.	NA	Fixed in release 04.1.01
65	04.1.00	04.2.00	2021-05-03	EAGLE20/30 EAGLE40-03 EAGLE40-07	OpenSSL vulnerabilities (CVE-2021-3449, CVE-2021-23841, CVE-2021-23840)	-	Fixed in release 04.2.00
66	03.5.00	04.2.01	2021-08-26	EAGLE20/30 EAGLE40-03 EAGLE40-07	ntpd vulnerability (CVE-2018-8956)	-	Fixed in release 04.2.01
67	03.5.00		2020-08-02	EAGLE40-03 EAGLE40-07	After reboot of IDS server, it could not trigger remote sensor in active Eagle device in case any remote sensor is not reachable.	While reboot of IDS server, make sure all the remote sensors are reachable.	To be fixed together with future maintenance release.
68	03.2.00	04.3.02	2021-12-06	EAGLE20/30 EAGLE40-03 EAGLE40-07	Unsupported 'ping answer' checkbox from VRRP Wizard needs to be removed.	-	Fixed in release 04.3.02
69	04.3.00	04.3.02	2022-05-09	EAGLE40-03 EAGLE40-07	Enabling IP address restriction operation over VPN breaks communication over VPN tunnel.	-	Fixed in release 04.3.02
70	02.0.01	04.2.01	2015-09-02	EAGLE20/30 EAGLE40-03 EAGLE40-07	It is not possible to add another Static Route with the same Network Destination	-	Fixed in release 04.2.01
71	04.0.00		2020-11-12	EAGLE40-03 EAGLE40-07	After adding static mac address to interface-1, same mac is getting learned to other interface-2 while traffic is send with same mac as source mac on interface-2	The behavior of static MAC filters in linux kernel is different from BCM switch. As this is linux default behavior, hence suggested to tolerate the same.	To be fixed in future release.



ID	Since	Fixed in	Date	Variant	Description	Workaround	Correction
72	03.4.00	04.3.00	2022-02-10	EAGLE40-03 EAGLE40-07	Busybox (CVE-2021-42373 .. CVE-2021-42386)	-	Fixed in Release 4.3.00
73	04.0.00	04.2.01	2021-03-25	EAGLE20/30 EAGLE40-03 EAGLE40-07	Usage of Outdated Cryptographic Methods	-	Fixed in release 04.2.01
74	04.2.00	04.3.00	2021-12-16	EAGLE20/30 EAGLE40-03 EAGLE40-07	uClibc (CVE-2021-43523)	-	Fixed in Release 4.3.00
75	03.2.00	04.3.02	2022-03-24	EAGLE20/30 EAGLE40-03 EAGLE40-07	Multiple security fixes	-	Fixed in release 04.3.02
76	04.0.00	04.4.00	2022-10-07	EAGLE20/30 EAGLE40-03 EAGLE40-07	Security Fix	-	Fixed in release 04.4.00
77	04.0.00	04.5.00	2022-11-04	EAGLE20/30 EAGLE40-03 EAGLE40-07	Security Fix	-	Fixed in release 04.5.00
78	4.3.00	04.4.00	2022-08-03	EAGLE40-03 EAGLE40-07	ARP Accept rule in L2 packet filter Bypass traffic through firewall.	-	Fixed in release 04.4.00
79	03.4.00	04.4.00	2020-11-05	EAGLE40-03 EAGLE40-07	System Off Bypass cannot be disabled	-	Fixed in release 04.4.00
80	04.2.00	04.4.00	2021-12-03	EAGLE40-03 EAGLE40-07	Incomplete SFP detail info	-	Fixed in release 04.4.00
81	04.4.00	04.5.00	2023-03-02	EAGLE20/30 EAGLE40-03 EAGLE40-07	Modbus DPI not working for VRRP Interfaces.	-	Fixed in release 04.5.00
82	04.3.02	04.6.00	2023-01-31	EAGLE40-03	1:1 NAT traffic drops observed after 2 weeks.	-	Fixed in release 04.6.00
83	04.0.00	04.5.00	2023-04-05	EAGLE20/30 EAGLE40-03 EAGLE40-07	Multiple OPC DPI fixes	-	Fixed in release 04.5.00
84	04.0.00	04.6.00	2023-04-05	EAGLE40-07	L3 relay is not supported for Vlan interfaces	-	Fixed in 04.6.00 Release
85	4.6.00	4.6.01	2023-07-07	EAGLE20/30 EAGLE40-03 EAGLE40-07	On enabled proxy ARP for VRRP interface, ARP response with VMAC is sent to all ARP request received on VRRP interface.	-	Fixed in release 04.6.01
86	04.5.00	04.7.00	2023-04-20	EAGLE20/30 EAGLE40-03 EAGLE40-07	Security Fix	-	Fixed in release 04.7.00
87	04.2.01	04.6.02	2023-09-19	EAGLE20/30	Persistent log file is not getting created under usb even when log file target is set as usb.	-	Fixed in release 04.6.02
88	03.2.00	04.6.02	2018-03-15	EAGLE20/30	VRRP announcements sent with physical MAC address	-	Fixed in release 04.6.02
89	04.7.00		2023-09-20	EAGLE20/30 EAGLE40-4F	Interface based MGMT-RMA rule is not working for Eagle30.	-	To be fixed in future release.
90	03.5.00	04.8.00	2023-08-18	EAGLE40-03 EAGLE40-07	Masquerading NAT does not work in combination with vlan based router interfaces when same vlan is assigned on multiple interfaces.	-	Fixed in release 04.8.00
91	03.2.00		2023-09-04	EAGLE20/30 EAGLE40-03	VPN Tunnel when unstable due to link fluctuation on switch causing memory leak.	-	To be fixed in future release.
92	03.0.00	04.7.00	2023-01-31	EAGLE20/30 EAGLE40-03 EAGLE40-07	FLM contains some fixed rule entries in factory defaults.	-	Fixed in release 04.7.00
93	03.5.00	04.8.00	2023-10-11	EAGLE20/30 EAGLE40-03 EAGLE40-07	Security Fix	-	Fixed in release 04.8.00
94	03.5.00	04.8.00	2023-09-20	EAGLE40-03 EAGLE40-07	Eagle40 interfaces are up before the configuration is loaded completely during reboot.	-	Fixed in release 04.8.00
95	04.2.00		2023-11-06	EAGLE20/30 EAGLE40-03 EAGLE40-07 EAGLE40-4F EAGLE40-6M	Security Fix: Device vulnerable to Slowloris DOS attack	-	To be fixed in future release.
96	04.8.00		2024-03-06	EAGLE40-03 EAGLE40-07 EAGLE40-4F	Event logs for L2 frame forwarding and Link flap operation not getting generate.	-	To be fixed in future release.
97	03.5.00	05.1.00	2023-06-20	EAGLE40-03	Copper SFP not working on Eagle device, requires reboot and plugin to work.	-	Fixed in release 05.1.01
98	03.5.00	04.8.00	2022-11-04	EAGLE40-03 EAGLE40-07 EAGLE40-4F	OSPF not enabled on interface after reboot	-	Fixed in release 04.8.00
100	04.5.00	05.0.00	2024-07-17	EAGLE40-07	Security improvements by updating expat to version 2.6.2.	-	Fixed in release 05.0.00
101	04.4.00		2024-09-06	EAGLE20/30 EAGLE40-03 EAGLE40-07 EAGLE40-4F EAGLE40-6M	Security Fix of IPSET Vulnerability	-	To be fixed in future release.
103	04.7.00	05.1.00	2024-05-03	EAGLE40-03	1. Secondary IP is not reachable post config save and reboot. 2. Clear config doesn't clear secondary IP.		Fixed in release 05.1.00
104	04.5.00	05.1.00	2024-06-12	EAGLE40-07	VLAN router interfaces are not coming up reliable after reboot	-	Fixed in release 05.1.00
105	04.3.02	05.1.00	2024-06-12	EAGLE40-07	Configuration cannot be deleted via sysMon1 for EAGLE40-07		Fixed in release 05.1.00