IQ Engine 8.2r11 Release Notes

Release date: August 27, 2021

Hardware platforms supported: AP122, AP122X, AP130, AP150W, AP230, AP245X, AP250, AP550, and AP1130

Management platforms supported: HiveManager Classic 8.2r2 and later

New Features and Enhancements

This release introduces the following new features and enhancements:

DNS Hardening: DNS components have been upgraded to protect against recently discovered vulnerabilities in some DNS-related services.

DTLS 1.2 Support: Devices running this release or later of IQ Engine now support DTLS 1.2 to secure CAPWAP tunnels. DTLS 1.0 is deprecated.

Security Hardening: This release hardens IQ Engine against fragment cache attacks, mixed key attacks, and frame aggregation attacks. This release also includes PHP 7.4, which address vulnerabilities in previous versions.

Known and Addressed Issues

Known Issues in IQ Engine 8.2r11

HOS-11615	An admin cannot add a new NAS (network access server) list unless the local RADIUS server is first disabled and then re-enabled.
HOS-11450	When tunneling wired guest traffic to a DMZ on an AP150W, the clients do not receive the appropriate IP address and tunneling is not successful. **Workaround**: Have clients connect to the wireless interfaces for tunneling guest traffic.
HOS-11138	Enabling Bonjour Gateway on an AP150W, AP122 or AP122X can cause those devices to report excessively high CPU loads. **Workaround**: Because Bonjour Gateway is a legacy feature, and is generally unnecessary, you can either disable Bonjour Gateway, or relocate Bonjour Gateways to a higher-powered access point such as an AP550.
HOS-11087	On the AP150W, if Client Monitor is performed against multiple clients concurrently, the access point occasionally loses the CAPWAP connection to ExtremeCloud IQ.
HOS-11004	Remote Packet Capture on the AP150W can only capture traffic from wireless interfaces.

Addressed Issues in IQ Engine 8.2r11

CFD-6318	IQ Engine did not recognize the CLI command string `no forwarding-engine proxy-ndp bypass-req-from-sta-to-external enable`.

Addressed Issues in IQ Engine 8.2r10

There are no addressed issues in this release.

Addressed Issues in IQ Engine 8.2r9

CFD-5569	Administrators could not configure a static WAN IP address using the NetConfig UI.
CVE-2020-16152 PSIRT-34 PSIRT-32	Attackers were able to exploit the web interface of devices running previous versions of IQ Engine to elevate privileges and to perform denial of service attacks.

Addressed Issues in IQ Engine 8.2r8

HOS-16364	Access points running IQ Engine 8.2r7 and earlier sometimes lost their radio calibration information.

Addressed Issues in IQ Engine 8.2r7

HOS-12634	Zero-wait DFS did not function properly in dual mode.
HOS-12259	Access points sometimes did not adjust transmit power in the presence of other access points.

Addressed Issues in IQ Engine 8.2r6

CFD-4059	ExtremeCloud IQ administrators could not fetch techdata files from access points.
CFD-4043	IQ Engine Access-Requests for RADIUS admin auth did not use the correct Service-Type value of 'Administrative'.
CFD-4014	A file system error caused APs to reboot.

Addressed Issues in IQ Engine 8.2r5

CFD-3905	AP130 Wifi1 radio (5 GHz) sometimes stopped transmitting or receiving, resulting in loss of client connectivity.
CFD-3892	Wi-Fi radios of AP250 and AP550 access points were reinitializing spontaneously.
CFD-3882	MDM enrollment of mobile devices was unsuccessful.
CFD-3858	When disabled, the embedded web server continued to respond on the mgt0 interface.
CFD-3836	Remote AP250 access points were unable to join domains.
CFD-3812	APs configured to use aggregate Ethernet interfaces required 802.11at power, but were reporting using only 802.11af power, which resulted in unstable client connectivity.
CFD-3695	After upgrading from IQ Engine 6.5r10 to IQ Engine 8.2r4, AP230 access points were spontaneously rebooting and reverting back to IQ Engine 6.5r10.

CFD-3687	AP230 access points were spontaneously rebooting without apparent cause.
CFD-3673	DFS was enabled on AP1130 access points, even when DFS was disabled in the radio profile.
CFD-3667	AP130 access points running IQ Engine 8.2r3 were rebooting spontaneously.
CFD-3599	AP250 and AP550 access points were exhibiting high CPU utilization when using GRE tunnels.
CFD-3574	Client devices were losing connectivity when connected to AP150W access points on the 2.4 GHz interface.
CFD-3561	CRC error airtime percentage appeared with the incorrect value.
CFD-3549	The login success page redirection URL was used for both *Login Successful* and *Registration Successful* results.
CFD-3528	EIRP power displayed the incorrect value.
CFD-3516	The voice call setup process was unsuccessful because of an ARP cache IP address mismatch.
CFD-3459	64-bit values queried for the 1.3.6.1.2.1.31.1.1.1.10.6 OID using SNMP were truncated, leaving only the low-order 32 bits.

Addressed Issues in IQ Engine 8.2r4

CFD-3513	User groups that existed within nested OUs were not properly added for LDAP server attribute mapping.
CFD-3511	When an admin entered the `show station` command with ARP proxy disabled, the IP address of client devices that were connecting with a static IP address appeared as 0.0.0.0.
CFD-3472	Some devices running spectrum analysis incorrectly reported interference sources.
CFD-3470	When iPhones attempted to reconnect to an SSID with auto-join disabled, the AP sometimes returned the following error instead of connecting to the SSID: Incorrect password for <ssid>.
CFD-3461	Some outbound traffic to international subnets contained the IP address of the AP as the source address.
CFD-3460	When WMM was disabled on an SSID, AP122, AP130, and AP230 access points, clients were unable to associate to the SSID.
CFD-3439	SNMP did not function properly after rebooting the device when the SNMP server was configured to use the domain name.
CFD-3414	UPA (Use Policy Acceptance) authentication did not work properly when also using PPSK.
CFD-3396	The default captive web portal IP address redirected users to the Cloudflare DNS website.
CFD-3376	After updating IQ Engine devices to IQ Engine 6.5r9a, some users could no longer authenticate using 802.1X.
CFD-3265	Fragmented DNSv6 packets were not forwarded to the Wi-Fi interfaces.
CFD-2999	When connecting to a PPSK SSID after self-registering, the UPA captive web portal did not appear.

Addressed Issues in IQ Engine 8.2r3

CFD-3349	When exporting tech data, AP122 access points did not generate `show station` output.
CFD-3294	Ocasionally, access points did not update successfully when static scanning channels were configured to include DFS channels.
CFD-3149	The Wifi0 interface sometimes did not respond properly to RTS frames sent by client devices.
CFD-3139	AP120 and AP230 access points sometimes spontaneously rebooted.
CFD-3129	In some cases, AP550 access points running IQ Engine 8.2r1 frequently rebooted.
CFD-2832	AP250 access points running IQ Engine 8.2r1were rebooting spontaneously.
CFD-2781	AP550 access points erroneously reported high utilization, which appeared in the ExtremeCloud IQ spectrum analysis displays.
CFD-2644	AP230 access points classified 802.1p traffic properly, but did not properly classify some DiffServ traffic.
HOS-12634	Zero-DFS did not function properly on AP150W, AP250, and AP550 access points running IQ Engine 8.2r1.
HOS-12259	APs running IQ Engine 8.2r1 sometimes did not detect neighboring devices running on other channels during background scanning.

Addressed Issues in IQ Engine 8.2r2

CFD-3208	When using self-registration with captive web portal, the captive web portal did not appear on client devices running Android 7.1 or later, preventing successful registration.
CFD-3181	IQ Engine devices did not properly respond to some Disconnect-Request and Change-of-Authorization packets.
CFD-3155	ID Manager users were unable to authenticate because IQ Engine was using an incorrect IDM Proxy address.
CFD-3140 CFD-3129	AP550 access points sometimes spontaneously rebooted.
CFD-3139	AP130 and AP230 access point sometimes spontaneously rebooted.
CFD-3103	The ExtremeCloud IQ PPSK import process did not import email addresses that use the .asia domain.
CFD-3102	In some cases, Disconnect-Request and CoA packets were not processed properly, resulting in persistent retries.
CFD-3061	The RADIUS Service-Type attribute was not set properly within Access-Request and Accounting-Request packets.
CFD-3042	IP-Policy Layer 7 IPv6 rules whose source address value was "any" did not function properly.
CFD-3035	Devices running IQ Engine 8.1 sometimes raised alarms in ExtremeCloud IQ when using RADIUS with attribute mapping.
CFD-3034	HPE/Aruba ClearPass did not function properly when MAC authentication was used.
CFD-3017	IP address byte order in Layer 7 log entries was reversed.
CFD-3015	ExtremeCloud IQ allowed an admin to enter a 32-character user profile assignment group name, but returned an error.

CFD-3001	AP550 access points were not drawing the correct PoE power from the PSE when LLDP was enabled.
CFD-2945	The AP150W did not correctly negotiate 802.3at power levels when using LLDP-MED.
CFD-2910	Devices using the Taiwan country code (158) did not support DFS.
HOS-13111	Under certain circumstances when using RADIUS-based authentication, some wireless clients did not complete DHCP negotiations successfully, and did not acquire an IP address.
HOS-12459	AP550 access points sometimes assigned Wi-Fi radio channels with insufficient separation.

Addressed Issues in IQ Engine 8.2r1a

CFD-3076	AP245X access points operating on the 2.4 GHz band were experiencing very high airtime utilization in some regions.
CFD-3039	AP245X access points running IQ Engine 8.2r1 sometimes stopped forwarding client traffic to the network, resulting in a loss of client connectivity.
CFD-2980	Clients connected to some APs running IQ Engine 8.2r1 were experiencing intermittent packet loss on the 2.4 GHz band.
CFD-2973	Some devices were able to connect to AP230 and AP330 access points, but not to AP250 access points with a similar configuration.
CFD-2924	AP250 access points running IQ Engine 8.1r2a were experiencing high CPU utilization.

Addressed Issues in IQ Engine 8.2r1

HOS-11248	For the AP150W, the rate limiting settings for Eth2 and Eth3 did not appear after running a `show running config` command.