

IQ Engine 10.0r10a Release Notes

Release date: December 20, 2020

Hardware platforms supported: Atom AP30, AP122, AP122X, AP130, AP150W, AP230, AP245X, AP250, AP510C, AP510CX, AP550, AP630, AP650, AP650X, AP1130, and XR600P

Management platforms supported: ExtremeCloud IQ 20.11.50.1 and later

Known and Addressed Issues

The following tables list known and addressed issues in IQ Engine 10.0.

Known Issues in IQ Engine 10.0r10a

HOS-16788	The displayed value of total data transmitted to a client does not match the displayed value of total data received by the clients.
-----------	---

Addressed Issues in IQ Engine 10.0r10a

CFD-5777	Some APs running IQ Engine 10.0r10 were experiencing wireless connectivity loss.
----------	--

Addressed Issues in IQ Engine 10.0r10

CFD-5569	Administrators could not configure a static WAN IP address using the NetConfig UI.
CFD-5552	The L7d service exceeded its memory allocation.
CFD-5525	Devices sometimes transmitted the same client trail information twice, resulting in duplicate rows in ExtremeCloud IQ.
CFD-5498	Client devices did not re-authenticate properly during roaming.
CFD-5460	Mobile clients were unable to authenticate through the captive web portal through some APs running IQ Engine 10.0r9a.
CFD-5448	AP650 access points could not reconnect to the network after a broadcast storm ended.
CFD-5396	Firewall rules did not upload properly to devices.
CFD-5387	AP250 access points were incorrectly generating CRC errors.
CFD-5340	AP650 access points sometimes falsely reported radar events when both radios were in 5 GHz mode.
CFD-5204	The radiusd service exceeded its memory allocation.
CFD-4608	Some APs became unresponsive during normal operation.
CVE-2019-3460 CVE-2019-3459 HOS-15307	Some versions of the Linux kernel were susceptible to allowing unauthorized access to attackers with sufficient physical access to establish a Bluetooth connection and transmit a special malformed packet.

Addressed Issues in IQ Engine 10.0r9b

CVE-2020-16152 HOS-15030	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 10.0r9a

CFD-4802	Administrators could not retrieve tech data for AP1130 access points running HOS 10.0r8.
CFD-4710	Client devices sometimes disconnected because the VLAN changed during user profile reassignment.
CFD-4671	Remote sites lost VPN connection to VGVA, requiring administrators to restart the IPsec session.
CFD-4641	AP650 access points sometimes initiated a system core dump, and then rebooted or became unresponsive.
CFD-4005	When the XR600 router was used as a Layer 2 VPN server, TCP sessions within the tunnel sometimes closed unexpectedly.

Addressed Issues in IQ Engine 10.0r9

CVE-2019-15126 HOS-15944	Broadcom access points and wireless clients were vulnerable to traffic decryption during a very short time window during the dissociation process.
-----------------------------	--

Addressed Issues in IQ Engine 10.0r8

CFD-4471	When an admin configured an SSID to drop all non-management traffic destined for the ap, users were unable to authenticate to the network using PPSK self-registration.
CFD-4470	Wildcard characters did not function properly in walled garden captive web portals when NAT was enable on a user profile.
CFD-4453	Disconnecting a client from a WPA3 SSID caused all other clients to disconnect.
CFD-4422	In the output of different commands, IQ Engine reported different values for the same transmit power parameter.
CFD-4398	BLE iBeacons were inconsistently reported in the AP650 iBeacon monitor list output.
CFD-4309	AP650 access points rebooted soon after Cisco phones connected.
CFD-4300	When some APs were configured for scheduled reboot, Wi-Fi interfaces were shut down, preventing clients from reconnecting after the reboot.
CFD-4245	AP630 and AP650 access points were dropping a high number of packets.
CFD-4242	Some internal running processes of AP630 access points became unresponsive.
CFD-4190	AP1130 access point were rebooting spontaneously.
CFD-4126	When NTLMv1 was disabled in Active Directory, some access points were unable to act as RADIUS servers using PEAP with MS-CHAP-v2 authentication.
CFD-4086	Network users were sometime assigned to incorrect VLANs and RADIUS attributes were used for classification.
CFD-4085	IQ Engine was reporting high interference to ExtremeCloud IQ.