# IQ Engine 10.0r9 Release Notes

**Release date**: June 19, 2020

**Hardware platforms supported**: AP150W

**Management platforms supported**: ExtremeCloud IQ 20.5.1.1 and later

## New Features and Enhancements

This release introduces the following new features and enhancements:

**Kr00k Vulnerability Mitigation**: This release fixes a known issue with Broadcom Wi-Fi clients. You can find additional information about the Kr00k vulnerability at the following URL:

https://nvd.nist.gov/vuln/detail/CVE-2019-15126

**Router Mode Support for AP150W**: Using that AP150W running IQ Engine 10.0r9 enables administrators to configure the AP150W to function as a router with many of the same routing capabilities as the XP200P. Running 10.0r9, the AP 150W also retains integrated Wi-Fi capabilities.

## Known and Addressed Issues

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

### Known Issues in IQ Engine 10.0r9

There are no known issues in this release.

### Addressed Issues in IQ Engine 10.0r9

| | |
|---|---|
| CVE-2019-15126<br>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. |