

## HiveOS 6.5r8a Release Notes

**Release date:** October 17, 2017

**Release versions:** HiveOS 6.5r8a

**Hardware platforms supported:** AP110/120, AP1130, AP121/141, AP130, AP170, AP230, AP320/340, AP330/350, AP370/390, SR2024, SR2024P, SR2124P, SR2148P

**Management platforms supported:** HiveManager 8.1r2 and later, and HiveManager NG 11.26.2 and later

---

### Changes in Behavior and Appearance

This release adds the following changes in behavior and appearance:

- HiveOS 6.5r8a mitigates the WPA2 key reinstallation attack commonly known as KRACK. For more information regarding this vulnerability, see <https://www.krackattacks.com/>. You can also find the Aerohive response to KRACK at <http://docs.aerohive.com/krack>.

---

### Known Issues in HiveOS 6.5r8a

The following known issues exist in HiveOS 6.5r8a.

#### Known Issues in HiveOS 6.5r8a

|          |  |
|----------|--|
| CFD-2622 | <p>Recent changes in Apple iOS used in iPhones and iPads can react poorly to the ACSP (Aerohive Channel Selection Protocol) behavior from 802.11n access points, resulting in iOS devices refusing to reconnect automatically to the advertised SSID, and logging a reason code 6.</p> <p><b>Workaround:</b> Implement a static channel plan, or configure the radio profiles so that channel scanning and selection occurs during a window of time when no client devices are connected and channels used by common interferers such as weather radar are excluded.</p> |
| CFD-2627 | <p>The recent WannaCry exploit caused many customers to disable SMBv1 on their Windows servers, which can prevent successful 802.1X connections by preventing access to the Active Directory data store.</p> <p><b>Workaround:</b> Re-enable SMBv1 on the AD servers, or implement Microsoft's NPS as a RADIUS server.</p>   |

## Addressed Issues

The following issues were addressed in the current and previous HiveOS releases.

### Addressed Issues in HiveOS 6.5r8

|           |   |
|-----------|---|
| HOS-12153 | Corrected an issues with the WPA2 standard that allowed for PTKs, GTKs, and IGTKs to be replaced during the four-way handshake. |
|-----------|---|

### Addressed Issues in HiveOS 6.5r8

|                      |  |
|----------------------|--|
| CFD-2652             | Portal APs were being incorrectly reported as mesh ports because AMRP was not recognizing and reporting brief changes to interface status.   |
| CFD-2639             | SNMP error counters were incorrect on an SR2024P switch.   |
| CFD-2633             | DNS query responses that were fragmented due to their large size were not reassembled when ALG was enabled, causing DNS queries to fail.   |
| CFD-2617             | After 200+ days of uptime during which they were mostly idle, some access points could get into a state where they would erroneously report their CPU utilization at 100%".                            |
| CFD-2557             | After adding a new network or new branch router, there was a substantial delay while the OSPF routing table was rebuilt in the HiveOS Virtual appliance (formerly known as CVG).                       |
| CFD-2539             | BR200 devices were not communicating with the SNMP server.   |
| CFD-2529<br>CFS-2429 | Client usage data displayed in various HiveManager NG pages was inconsistent.  |
| CFD-2488             | SSID data displayed in the dashboard was inconsistent or incorrect.  |
| CFD-2460             | AP230s using the 6.5r6 image were continually rebooting.   |
| CFD-2309             | On 802.11ac APs ACSP behavior sometimes triggered BSS avoidance in iOS clients.  |
| HOS-9300             | Medium strength ciphers for SSL, previously retained for backward compatibility, have been removed from HiveOS. HiveOS no longer accepts or initiates connections with TLS versions earlier than v1.1. |

### Addressed Issues in HiveOS 6.5r7

|           |  |
|-----------|--|
| CFD-2385  | Manually-configured RADIUS proxies were missing realm names which caused AP authentication to fail periodically.                                     |
| CFD-2264  | Some router subnets were not being advertised by the OSPF.   |
| CFD-2248  | For the AP130 and AP230 the 802.11e load element was always present even when WMM (Wi-Fi Multimedia) was disabled.                                   |
| CFD-2245  | The Available Admission Capacity was always 0.   |
| CFD-2193  | AP121s were flooding the network with MDNS traffic.  |
| CFD-2118  | Acct-Session-Id and Acct-Multi-Session-Id were missing from RADIUS Access-Request packets  |
| CFD-2063  | Added basic Acct-Multi-Session-Id support for Disconnect-Request (and CoA), for better interoperability with systems that perform RADIUS accounting. |
| CFD-1921  | Packet MTU increased when the packet reached the CVG tunnel0 interface.  |
| HOS-10073 | The EU country code was added to SKUs for AP121, AP141, BR200, AP130, and AP230.   |

|          |  |
|----------|--|
| HOS-9885 | Addressed CVE-2017-6214.   |
| HOS-9447 | When 802.1x authenticated users roamed from an AP330 or AP370 to AP230, the client's class attribute was not shared, causing incorrect firewall rules to be applied. |

## Addressed Issues in HiveOS 6.5r6

|          |  |
|----------|--|
| CFD-2200 | Clients who were exempted from registering on an external captive web portal because they were using MAC-based authentication were unable to connect.                  |
| CFD-2195 | An invalid Acct-Authentic attribute has been removed from Accounting-On/Accounting-Off-Request packets.  |
| CFD-2151 | The length of the user name in the client usage report has been expanded from 32 characters to 128 characters to prevent the return of erroneous data.                 |
| CFD-2121 | PPSK revocation was not taking effect.   |
| CFD-2120 | PPSK users with revoked privileges were still able to connect after an AP was rebooted.  |
| CFD-2119 | AP130 devices were returning invalid AIFSN values in response to probes.   |
| CFD-2094 | HiveOS was not changing the user profile based on RADIUS CoA (change of authentication).   |
| CFD-2003 | Connection to the corporate network was lost due to virtual appliances and routers losing OSPF routes.   |
| CFD-1965 | The client monitor log was displaying an incorrect RSSI value.   |
| CFD-1964 | Voice traffic using a Cisco 8841 was being routed on the data VLAN.  |
| CFD-1815 | AP370 devices were unexpectedly rebooting because they were running out of buffers when too many clients were connected, which caused inconsistent internal variables. |
| CFD-1790 | Improvements were made to avoid false radar detection by the AP230.  |
| HOS-9276 | An MIC verification failure in TKIP that was disconnecting AES users has been fixed.   |
| HOS-9035 | RADIUS Class attributes could cause authentication issues in an environment with different models of AP.   |
| HOS-8330 | The UPID was incorrectly assigned based on the RADIUS returned attribute for a PPSK with MAC authentication enabled.   |
| HOS-8318 | An error in the LLDP-PoE code logic has been addressed.  |

## Addressed Issues in HiveOS 6.5r5

|          |   |
|----------|---|
| CFD-1947 | The AeroScout server was not able to process data sent by a tag through an AP230.   |
| CFD-1928 | Previously HiveOS misinterpretations of an NTP server message intended to signify correct time not available, or not yet set on the server resulted in time stamps in 2036. This also affected services such as ID Manager and IPSec tunneling to fail. |
| CFD-1905 | SNMP traps emitted from an AP230 with embedded IP addresses would have the IP addresses reversed.   |
| CFD-1860 | AP IP sessions increased significantly after a classifier map (CM) was pushed to the configuration.   |

|                  |  |
|------------------|--|
| CFD-1833         | The show vpn ike sa and show vpn ipsec sa commands were not displaying data for the CVG.   |
| CFD-1820         | DHCP packets were using invalid client MAC address for Bonjour Gateway.  |
| CFD-1811         | The transmit (Tx) power for AP130 devices was displayed as 31 dBm after a reboot.  |
| CFD-1805         | There were inconsistencies in the show ACSP neighbor and show hive neighbor RSSI output.   |
| CFD-1801         | A lockup was causing AP370 devices to reboot.  |
| CFD-1798         | MAC auth and 802.1x auth were not using the same action when the user-profile-mapping function was enabled.  |
| CFD-1795         | RADIUS class attributes were no longer available after a BSS transition.   |
| CFD-1759         | Legacy clients could not be authenticated with EAP (LEAP).   |
| CFD-1719         | The list of friendly APs that appears on non-DA APs did not include all of the information that appeared on the list for DA APs.   |
| CFD-1706         | APs were incorrectly recognizing themselves as rogues.   |
| CFD-1195         | AP121 devices were running out of memory and returning the following message: "amrp2: page allocation failure. order:3, mode:0x20".  |
| HOS-7525 (14158) | Under certain circumstances, hardware TCP checksums were incorrectly calculated, resulting in the AP320 and AP340 corrupting forwarded frames.   |
| HOS-7478         | Weak (96-bit and less) ciphers and the SHA-1 MAC algorithm, retained for backwards compatibility with old client devices that did not support modern crypto ciphers or MAC algorithms, have been removed, to prevent false positives from security scanners. |
| HOS-7312         | The event-timestamp was missing on the Accounting-On, Accounting-Off, and Start forms of the Accounting-Request packets.   |
| HOS-7311         | The Acct-Delay-Time RADIUS attribute was missing on Accounting-Request packets.  |
| HOS-7310         | Accounting-Off Accounting-Request packets were not being sent by HiveOS when a reboot command was issued.  |
| HOS-7220         | Self-signed certificates, used for securing HTTPS access to the HiveOS device, have been updated to use the SHA-256 algorithm for signing.   |
| HOS-7134         | Configuring the "Redirect to the initially requested page" option with the access web server's page as the first URL created an endless loop of login requests.  |
| HOS-6261         | The Filter ID was unable to assign a user profile correctly.   |

## Addressed Issues in HiveOS 6.5r4

|          |  |
|----------|--|
| CFD-1750 | UDP CAPWAP connections would sometimes close and then reopen over HTTP. When this occurred, client devices could not communicate with the network.                                 |
| CFD-1722 | After upgrading AP230 access points to HiveOS 6.5r3, some client devices would intermittently not receive DHCP offers that were being sent by the DHCP server.                     |
| CFD-1703 | The SR2024P switch operating in router mode becomes unresponsive during bootup when using the Huawei E8372 modem as the backup WAN port and the primary WAN connection is removed. |
| CFD-1693 | The four-way handshake process was sometimes unsuccessful because of unexpected WPA key data returned by the supplicant.   |

|          |   |
|----------|---|
| CFD-1686 | SR2024P switches were reporting the IP address octets of connected hosts to HiveOS in reverse order.  |
| CFD-1647 | Macbooks sometimes did not process the 802.11h power constraint value correctly, which resulted in a transmit power setting that was too low. This version of HiveOS introduces Client Transmit Power Control, now disabled by default, which instructs the client device to match the AP transmit power. |
| CFD-1581 | The RADIUS failover process was taking several seconds, causing some clients to disassociate, and then be unable to re-associate after the process completed.   |
| CFD-1550 | VPN tunnels being negotiated by the BR200-WP router would sometimes take several minutes because the xauth-request packet was not received when expected.   |
| CFD-1502 | BR200 routers sometimes reported an incorrect vendor ID to HiveOS during the configuration upload process, which resulted in HiveOS reporting an error and preventing a successful configuration upload.  |
| CFD-1374 | Clock drift of some HiveOS devices would sometimes create sufficient disparity to cause VPN tunnels to close and then need to be renegotiated, producing data transfer interruptions.   |
| CFD-1383 | After upgrading to HiveOS 6.6r1, devices were unable to execute the DHCP option commands properly.  |
| HOS-6723 | Although there is no method to exploit CVE-2015-7547 within HiveOS, Aerohive has updated HiveOS to prevent false positive responses being generated by security software.   |

## Addressed Issues in HiveOS 6.5r3a

|          |   |
|----------|---|
| HOS-5200 | Aerohive devices demonstrated small, but constant packet loss in active VoIP sessions when there was simultaneous lower-priority traffic, for example, background file transfers and streaming video. |
|----------|---|

## Addressed Issues in HiveOS 6.5r3

|                      |   |
|----------------------|---|
| CFD-1331<br>CFD-1245 | The VPN daemon running on the HiveOS Virtual Appliance spontaneously restarted, causing all active VPN tunnels to reset unexpectedly.   |
| CFD-1289             | The AP230 was reporting the incorrect transmit and receive airtime counts.  |
| CFD-1111             | When authenticating through a HivePass captive web portal, the user profile was assigned an incorrect user profile attribute value.   |
| CFD-1097             | The byte order of the IP address was reversed as reported by SNMP v2C traps on the AP230, which resulted in the apparent failure of applications due to firewalls dropping packets with bad reverse IP addresses.             |
| CFD-897              | NetConfig UI reported a validation error when a password was configured to end in the letter z.   |
| HOS-2635             | On Aerohive SR-series switches, performing an SNMP walk (snmpwalk) resulted in an error.  |
| HOS-1680             | The Troubleshooting tool within HiveOS NG was incorrectly reporting that clients configured an incorrect static IP address or gateway although the clients were properly configured and functioning correctly on the network. |

2017 ©Aerohive Networks, Inc.

Aerohive is a U.S. registered trademark of Aerohive Networks, Inc.