Version 6.0.0 introduced the following:
Release Month-Year: March 2016

1. Updated Linux OS build. All new compiled from bootstrap. The OS is now 64 bit. DHCPatriot systems prior to model 2008-x may not be compatible.

2. DHCPatriot news on the home screen (Screen you see upon login to the web administration interface) is now pre-loaded. Previously, the news would be loaded at the time of display. This could cause issues if there was no network connection available or DNS servers were not available for some reason (such as at install time). Now, it will just immediately display either old news or a message that news could not be retrieved.

3. Search Sessions now has a view logs link as appears in View Authenticated Users for quick searching logs of the mac address of the session.

4. Device import now restarts DHCP upon a successful upload. Previously, the device import did not trigger a restart of DHCP as it should have.

5. Updated NTP to 4.2.8p4 to mitigate the KOD exploit that is a DoS attack on the NTP server.

6. Repaired a bug in Standard DHCP Actions -> TFTP File Maintenance that prevented filenames with spaces or other special characters from being viewed or deleted.

7. OUI lookup previously used an external page: standards.ieee.org Now uses internal database as that external tool is somewhat unreliable.

8. Previous change to remove check if user is online before allowing authentication has been reverted. The reason for this is that it causes to many problems with strange sessions that make no sense and can even cause sessions to continue in someone else's name.

9. View Authenticated Users has had several columns that had data defined inside of paragraph tags redefined to span tags to facilitate easier copy and pasting.

10. Repaired a problem where Auth DHCP Actions -> Authorize Customer did not honor network specific settings when authenticating with something other than the DEFAULT RADIUS server. For example, if DEFAULT was set to strip @domain, and a network specific setting was to NOT strip @domain, the Authorize Customer would ignore this override. It now correctly mashes the settings as is done throughout the rest of the system.

11. Enhanced log messages that appear when the DHCPatriot system gets behind processing events. It now shows how many KB/MB it is behind as well as an approximate amount of events.

12. Enlarged the pop-up screen for graphs so that all major browsers show the graphs without scroll bars.

13. A note on uptime via SNMP: Please use the hrSystemUptime (1.3.6.1.2.1.25.1.1.0) instead of sysUpTimeInstance (1.3.6.1.2.1.1.3.0) when getting uptime from the DHCPatriot system. The latter reports only how long snmpd has been running while the former reports the actual time that the system has been running.

14. VRRP previously required an undocumented restart if the address was changed. It now recognizes that the address has changed and automatically removes the old address and uses the new address.

15. Addressed a possible inflation in DHCP QPS count. If a system was exceptionally busy, it was possible for the system to count more DHCP QPS than occurred in the current 5 minute period then divide by 300 seconds thusly inflating the QPS for that period.

16. DHCP dont-use-fsync option has been added. This is strictly for performance in certain situations. This should not be used without a full understanding of what the implications are, which are noted with the setting. For the most part, this option should only be used by FNGi personnel.

17. A setting has been added to System Configuration -> General Setup that allows hiding of Shared Network from the list views on the Sticky IP, Exclude IP, Users Using Multiple IPs and Hijacked IP function pages. This is necessary on some systems for performance reasons on those screens. Particularly if there are a large number of entries on any of those screens.

18. Added Shared Network info to the lists on Exclude IP, Users Using Multiple IPs and Hijacked IP function pages. This can be turned off in System Configuration -> General Setup if it causes performance issues.

19. Added remote syslogging capability. To enable this, go to System Configuration -> General Setup and place an IP address to log to in 11) Remote Syslog IP (optional). DHCP server and general logs (like available under System Configuration -> System logs) will be sent to the syslog server.

20. Added Misc DHCP Values to Static DHCP subnet config. Did not add Pool DHCP Values here as there is no pool for Static DHCP subnet. This box works the same as the others. Place DHCP configs in here that work inside the subnet{} blocks on ISC DHCP. These configs will be placed inside the relevant static subnet{} block in the config.

21. Added Misc and Pool DHCP Values to Unauthenticated subnet config. Place DHCP configs in here that work inside the subnet{} and pool{} blocks on ISC DHCP. These configs will be placed inside the relevant static subnet{} and pool{} blocks in the config.

22. Added Misc and Pool DHCP Values to Authenticated Dynamic subnet config. Place DHCP configs in here that work inside the subnet{} and pool{} blocks on ISC DHCP. These configs will be placed inside the relevant static subnet{} and pool{} blocks in the config.

23. Added Misc DHCP Values to Authenticated Static subnet config. Place DHCP configs in here that work inside the subnet{} blocks on ISC DHCP. These configs will be placed inside the relevant static subnet{} blocks in the config.

24. Added a mass delete of suspended users in Auth DHCP Actions -> Built-in Authentication: User Maintenance. The delete suspended users link appears if there are suspended users. Once the delete is performed, a CSV of the deleted users is saved. This CSV can be downloaded and re-imported via Auth DHCP Actions -> Built-in Authentication: User Import if a mistake was made. Also, the CSV will remain unless it is removed. Remove and download links appear if the CSV exists. Only one CSV is kept. If more suspended users are removed at a later time, the CSV is replaced with a newer one.

25. API: Added mass suspend of authenticated devices by username. This would be analogous to accessing Auth DHCP Actions -> Suspend User and clicking "Suspend Multiple Users". Access the API feature by submitting to a URL similar to the following:

    - https://patriot.network1.net/cli/?function=AuthMassSuspend&username=apiuser&password=apipass¬e=This%20Would%20Be%20A%20Note
    - POST data must be sent containing the list of usernames for which you want devices suspended. There should be one username per line.

26. GLIBC patched for CVE-2015-7547.