1. BUG: A new algorithm has been developed that should help with a recent bug where new DHCPatriot systems databases would not be synchronized properly when the customer set them up initially.
2. BUG: A problem has been corrected where it was impossible to ping or trace to an IPv6 address as : characters could not be entered in the menu interface accessible via ssh or serial console for system configuration.
3. BUG: Fixed a problem where, under certain conditions of sorting columns clicked, and then subsequent activation of functions would cause sorting to break on some reports throughout the GUI. Thats a little vague, but it was widespread when it happened but also rare requiring a certain series of clicks to activate the bug.
4. BUG: Corrected a problem where DHCPv6 prefix delegations (both pre-auth and normal) allowed deleting a prefix delegation subnet even if it was in use. This caused a crash upon subsequent DHCP messages as the subnet no longer existed and therefore information about it could not be found. Now, the 'disable' link should be used first to empty the prefix delegation subnet. Then 'delete' may be used.
5. BUG: Corrected a problem where a suspended device in DHCPv6 that was also set to have a sticky IP address by DUID match would generate an error that the match type was unknown when really, the match shouldn't be made because the device is suspended.
6. BUG: Corrected math for the total lines in the DHCPv6 -> View Address Usage. The total lines were adding IPs in use from the subnet to the delegated prefix lines to get total lines. This is fine, however there were no available lines to add from the subnets, only from the delegated prefix. Therefore it might show over 100% in use on the total lines. The change we made is to stop adding the available and computing % in use for the total lines as those numbers were irrelevant since they were adding things of mixed type. It does still add the total of IPs and delegated prefix that are in use.
7. BUG: Delete, under System Configuration -> Captive Portal, did not work properly after changes to that function in 6.4.0. It was possible to delete Captive Portal configurations that were in use. It was also sometimes impossible to delete ones that it should have been possible to delete. This was because the delete mechanism had not been made aware of the changes and was still operating under the old method.
8. BUG: It was possible to delete in use Authentication server definitions. The DHCPatriot now, correctly, won't allow the removal of authentication server definitions that are in use.
9. BUG: It was previously possible to circumvent the limits on only searching for 24 hours (with no other search parameters present) on various reports by entering a * in a field that caused the limit to be removed (example: username in the report Auth DHCP Reports -> Search Sessions). This loophole has been closed. It is no longer possible to enter a * in a field with no other text.
10. BUG: Previously, in System Configuration -> General Setup, if there was an error on submission of edits and there were things that needed to be escaped in any of the text boxes on the screen, the escape characters would appear in the text boxes and cause all kinds of problems. This has been corrected and the escape characters are now stripped.
11. NEW: Changed the 'RADIUS server (optional)' box under Auth DHCP Actions -> Authorize Customer and DHCPv6 (IPv6) -> Authorize Device to only show one entry per RADIUS server grouping. Previously, it would show one entry per shared network definition. This would get confusing because there were so many entries shown. This new method should be fine as a descriptive name can be used for the RADIUS server grouping that will show up in this box alerting tech support or whoever to which one should be used.
12. NEW: Set 'Show option 82 inline' in 'Auth DHCP Reports -> Search Sessions' and 'Standard DHCP Reports -> Search Sessions' as well as 'DHCPv6 (IPv6) -> Search Sessions' 'Show option 18/37 inline' to stay checked if it was checked previously via a cookie. Some customers wanted this to default to checked but we didn't want to make that change for everyone so the cookie is a good compromise.
13. NEW: All of the search sessions, 'Auth DHCP Reports -> Search Sessions' and 'Standard DHCP Reports -> Search Sessions' as well as 'DHCPv6 (IPv6) -> Search Sessions', have been set to allow searching of more than 24 hours if any of the search parameters are provided (excluding date/time and display preferences, of course).
14. NEW: SSH now has a delay on bad authentication. It will accept three bad passwords an average of three times per minute. This is to prevent brute force attempts in the case of overly permissive firewall rules.
15. NEW: A new setting has appeared under 'System Configuration -> General Setup' called '11) Send Timezone to DHCP Clients (optional)'. If enabled, this causes the timezone under '10) Default Timezone (optional)' offset to be sent to the DHCP clients if they ask for it. Previously, the timezone offset sent to DHCP clients was always UTC.

16. NEW: Changed the name of form fields on any functions in the GUI (that weren't the actual authentication page) to not be called username / password so that the contents of such fields would stop being saved and auto-filled in the various browsers.
17. NEW: Changed the name of the username and password fields on the captive portal login screen so that various web browsers would stop offering to save passwords. It doesn't make any sense to save passwords there as the site that it would save the password for would not be the DHCPatriot itself, but rather for nfl.com or where ever they were trying to go. Also removed the text hints saying username and password in the boxes as they did not work properly anymore due to these changes. They were unneeded as the words are to the left of the boxes anyway.
18. NEW: You can now enter a * in the mac address field on Standard DHCP Reports -> Search DHCP Logs and Auth DHCP Reports -> Search DHCP Logs to search for a partial match. Please note that if you do use an * in the mac address, then you MUST use this mac address format: xx:xx:xx:xx:xx:xx as no other format (such as xx-xx-xx-xx-xx-xx) will work. For example: while 52:54:00:27:04:0* may give results, 52540027040* will not.
19. NEW: Auth DHCP Actions -> Suspend User now allows longer notes to be set for the suspension so that more complicated messages can be sent to the customer. The previous limit was 256 characters. The new limit is 64k. There is now a textarea instead of an input box for the notes field as well.
20. NEW: DHCPv6 (IPv6) -> Suspend Auth Device now allows longer notes to be set for the suspension so that more complicated messages can be sent to the customer. The previous limit was 256 characters. The new limit is 64k. There is now a textarea instead of an input box for the notes field as well.
21. NEW: In Auth DHCP Reports -> View Authenticated Users, if a device is suspended, a [-] link appears next to the word "SUSPENDED". Clicking this link will attempt to unsuspend the device.
22. NEW: In Auth DHCP Reports -> View Authenticated Users, a [+] link appears next to the username and the MAC address (MAC only if not currently suspended). Clicking this link will show the suspend user dialog in a popup window. Either the username or the MAC address will be pre-filled depending which [+] was clicked.
23. NEW: In DHCPv6 (IPv6) -> View Authenticated Users, if a device is suspended, a [-] link appears next to the word "SUSPENDED". Clicking this link will attempt to unsuspend the device.
24. NEW: In DHCPv6 (IPv6) -> View Authenticated Users, a [+] link appears next to the username, the MAC address (MAC only if not currently suspended and it exists), and the DUID (only if not suspended) Clicking this link will show the suspend user dialog in a popup window. Either the username, DUID or the MAC address will be pre-filled depending which [+] was clicked.
25. NEW: Lets Encrypt (https://letsencrypt.org/) support has been added. This can be enabled in the GUI: System Configuration -> Custom Web Certificate. Turning this support on will require a valid email address and FQDN (https://en.wikipedia.org/wiki/Fully_qualified_domain_name) that resolves to the DHCPatriot system. Enabling this will overwrite any other certificate that has been added to the system with the certificate retrieved from the Lets Encrypt service.
26. NEW: It is now possible to mark a dynamic DHCPv6 subnet to allow only known clients if it is not part of an authenticated subnet in DHCPv6 (IPv6) -> Dynamic Subnet. Adding clients to the system under DHCPv6 (IPv6) -> Known Client will give them access to subnets marked as only known client subnets.
27. NEW: Disabling global NTP servers setting has been exposed. Previously, the DHCPatriot would set NTP servers to be given to the DHCP client to its own IP addresses. There was no way to turn this off. Some customers needed to be able to not provide any NTP servers via DHCP so that they could manually set NTP servers on devices or set them via other methods which the inclusion in DHCP kept overriding. This setting: 'Disable DHCP Global NTP' in 'System Configuration -> General Setup' will remove the NTP server setting all together. Shared Network specific NTP server settings will still be delivered to the client, however.
28. NEW: The session cookie is now restricted to samesite for enhanced xss and csrf protection.
29. NEW: CSRF protection implemented in all forms.
30. NEW: To facilitate one-off routing requirements or really any other non-standard things, we have implemented a file called AfterBoot in non-volatile storage. We can place shell commands or scripting in this file. The file is executed as the last thing upon boot. This is sort of like the unix System V concept of rc.local.
31. NEW (API): A new API function has been added that allows the password to be set arbitrarily for an authenticated DHCPv4 user. This could be used as part of a strategy when password changes are implemented to prevent the user from having to log on at the captive portal again sometime later. Please note that the password will be changed for ALL devices that match the submitted username regardless of currently online status or suspended status. If there is possible ambiguity in your usernames attached to the devices, be sure and

keep that in mind before using this API function.
The URL for the API is:
https://patriot.[domain]/cli/index.php?
username=[apiuser]&password=[apipass]&function=NewPass&user=[usertochange]&newpass=[newpass]
example: https://patriot.alpha.network1.net/cli/index.php?
username=apiuser&password=apipass&function=NewPass&user=windows&newpass=t8s9AF3PqA

32. NEW: (API): It is now possible to set the permission level required to access API calls. The default is level 6. The level may be adjusted on the various API calls in System Configuration -> Set API Permissions. This works similarly to System Configuration -> Set App Permissions.
33. NEW: It is now possible to restrict dynamic subnets (IPv4 auth and standard as well as IPv6) from having sticky IPs assigned from them. Simply place a checkmark in 'Restrict Sticky IP Address' under the corresponding subnet. This will cause it to be impossible to allocate new sticky IPs from that subnet but will not affect existing assignments.
34. NEW: (API): BASearchCustomers now supports &JSON=true to enable a JSON return of the results instead of XML.
35. NEW: (API): dhcplogs now supports &JSON=true to enable a JSON return of the results instead of XML.
36. NEW: (API): GetNetworkConfig now supports &JSON=true to enable a JSON return of the results instead of XML.
37. NEW: (API): KnownClient now supports &JSON=true during the LIST action to enable a JSON return of the results instead of XML.
38. NEW: (API): Ping now supports &JSON=true to enable a JSON return of the results instead of XML.
39. NEW: (API): SearchAuthDevices now supports &JSON=true to enable a JSON return of the results instead of XML.
40. NEW: (API): SearchSessions now supports &JSON=true to enable a JSON return of the results instead of XML.
41. NEW: (API): StaticIPassign now supports &JSON=true during the LIST action to enable a JSON return of the results instead of XML.
42. NEW: (API): StickyIPs now supports &JSON=true during the LIST action to enable a JSON return of the results instead of XML.
43. NEW: (API): Trace now supports &JSON=true to enable a JSON return of the results instead of XML.
44. NEW: DHCPv6 Sticky IP and Delegated Prefix Assignment via RADIUS attributes now supported. Sticky IP address assignments can be sent in RADIUS attribute 168 "Framed-IPv6-Address". Sticky Delegated Prefix can be sent in RADIUS attribute 123 "Delegated-IPv6-Prefix". These attributes would need to appear in the access-response packet. They will be ignored if the result is not access-accept. The presence of these attributes will cause the DHCPatriot to assign these to the username that just authenticated. Either attribute or both may be present and the assignment will happen according to which is present. Be sure to use a unique username per device if you need to assign multiple addresses. Also be aware that all devices authenticated to that username will receive the assignments. The assignments can be removed on the DHCPatriot under DHCPv6 (IPv6) -> Sticky Assignments. Please note that if they are still assigned in RADIUS, that the next time one of the user's devices authenticates that the assignments will return.
45. NEW: Open-VM-Tools (https://github.com/vmware/open-vm-tools) now supported for VMware installs.