

RELEASE NOTES  
**GreenRADIUS UPDATE**  
**v4.1.6.7**

RELEASE DATE  
APRIL 1, 2020



### NOTES

- a. This GreenRADIUS update can only be applied to v4.0.2.2 or later.
- b. A minimum of 4GB RAM is recommended for this update to be applied successfully.
- c. Before applying updates, we recommend creating a snapshot of the GreenRADIUS VM in your virtualization server environment that can act as a backup.
- d. The update process may take about 10 to 15 minutes, and processing of authentication requests may be affected for some time during this process.

### STEPS TO APPLY THE UPDATE

1. Download the [update v4.1.6.7 zip file](#) (md5 = 2560663551672e9db0498938f507e083). Extract it, and it will result in a folder "GreenRADIUS\_4167\_Update"
2. Copy this folder onto the GreenRADIUS host in /home/gradmin using a client like scp or WinSCP
3. Log in to GreenRADIUS over ssh
4. Run the following commands:
  - a) `$ cd /home/gradmin/GreenRADIUS_4167_Update`
  - b) `$ sudo chmod +x install_update.sh`
  - c) `$ sudo sh install_update.sh`
5. The system and application components will be updated. After a successful update, a prompt will be shown to reboot the system. Type "y" to reboot the system to complete the process.
6. After a successful update, it is recommended to clean up the new directory created for this update process.
  - a) `$ sudo rm -rf /home/gradmin/GreenRADIUS_4167_Update`



### Ubuntu Vulnerabilities Patched

1. USN-4305-1 - ICU vulnerability
2. USN-4300-1 - Linux kernel vulnerabilities

### ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v4.1.5.6

1. A new report of inactive users who have not authenticated with the second factor successfully during the reporting period has been added. It can be run on demand, scheduled, and emailed to the configured email address.

### Questions? Contact us

support@greenrocketsecurity.com  
1-888-793-3247 -or- +44 808 234 6340