RELEASE NOTES

GreenRADIUS UPDATE v4.1.5.6

RELEASE DATE
MARCH 3, 2020

GreenRocket Security

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 v4.1.5.6 zip file (md5 = a03b35318b6815d0c96925fd7fcecf76). Extract it, and it will result in a folder "GreenRADIUS_4156_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_4156_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_4156_Update
```

Ubuntu Vulnerabilities Patched

1. USN-4284-1 – Linux kernel vulnerabilities
2. USN-4287-1 – Linux kernel vulnerabilities
3. USN-4285-1 – Linux kernel vulnerabilities
4. USN-4274-1 - libxml2 vulnerabilities
5. USN-4269-1 - systemd vulnerabilities
6. USN-4263-1 - Sudo vulnerability
7. USN-4253-2 - Linux kernel (HWE) vulnerability
8. USN-4256-1 - Cyrus SASL vulnerability

Questions? Contact us

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

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v4.1.4.5

1. Removed docker sock exposure
2. Strengthened validation in GRS APIs
3. Re-factored database access methods to defend against SQL injections
4. Updated Yubico OTP validation server to address SQL injection vulnerability
5. Fixed returning of group information in RADIUS responses in a few cases for vendor specific attributes (VSA) configuration setting
6. Added lockout mechanism for invalid authentication attempts