RELEASE NOTES

GreenRADIUS UPDATE v4.2.2.2

RELEASE DATE
DECEMBER 3, 2020

NOTES

a. This GreenRADIUS update can only be applied to v4.1.3.4 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 v4.2.2.2 zip file (md5 = 27fa9e3f808db3b9e1641cb1562168d4). Extract it, and it will result in a folder "GreenRADIUS_4222_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_4222_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_4222_Update`

VULNERABILITIES PATCHED

1. USN-4635-1 - Kerberos vulnerability
2. USN-4628-2 - Intel Microcode regression
3. USN-4627-1 - Linux kernel vulnerability
4. USN-4608-1 - ca-certificates update
5. USN-4602-1 - Perl vulnerabilities
6. USN-4593-1 - FreeType vulnerability
7. USN-4591-1 - Linux kernel vulnerabilities
8. USN-4582-1 - Vim vulnerabilities
9. USN-4581-1 - Python vulnerability
10. USN-4576-1 - Linux kernel vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v4.2.1.1

1. The configured OTP Prompt Text is now displayed for RADIUS authentication requests when OTP Input Method is set to Prompt For OTP
2. Fixed an issue that caused authentications to fail if temporary tokens contained special characters | or #
3. Fixed an issue that caused authentications to fail over RADIUS if passwords contained special characters " or \

Questions? Contact us

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