RELEASE NOTES
GreenRADIUS UPDATE v5.2.14.14

RELEASE DATE
DECEMBER 30, 2024

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v5.2.12.12 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 GreenRADIUS update v5.2.14.14 zip file (md5 = 54c7c56482cdacc911485a6d82a9aeb8, sha256 = c46110e02b741129be75f4141048812d467e85e3826c8f3f84f995f71f2fd8ae) Extract it, and it will result in a folder "GreenRADIUS_521414_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_521414_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_521414_Update

VULNERABILITIES PATCHED

1. USN-7117-2 - needrestart regression
2. USN-7131-1 - Vim vulnerability
3. USN-7117-3 - needrestart regression
4. USN-7145-1 - Expat vulnerability
5. USN-7149-1 - Intel Microcode vulnerabilities
6. USN-7154-1 - Linux kernel vulnerabilities (AWS)
7. USN-7162-1 - curl vulnerability
8. USN-7167-1 - Linux kernel vulnerabilities (AWS)
9. USN-7174-1 - GStreamer vulnerability

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v5.2.13.13

1. An enhanced version of our LDAP Authenticator Module is available. This facilitates integrations with applications such as SolarWinds.

2. Old Docker images are now automatically removed when the update is installed, helping to optimize disk space usage

3. Addressed an issue that caused high disk utilization on GreenRADIUS instances with a high number of login attempts

4. Fixed an issue that prevented tokens from being unassigned on the Users/Groups tab in certain scenarios

5. Fixed an issue where scheduled reports were not being sent via email when the configured SMTP server did not have TLS enabled

6. Fixed an issue where the temporary token feature did not work as expected when the Login Name Identifier was "userPrincipalName"

Questions? Contact us

support@greenrocketsecurity.com
1-888-793-3247