RELEASE NOTES

GreenRADIUS UPDATE v4.5.9.9

RELEASE DATE

MARCH 30, 2023

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v4.4.6.6 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.

VULNERABILITIES PATCHED

1. USN-5964-1 - curl vulnerabilities
2. USN-5963-1 - Vim vulnerabilities
3. USN-5960-1 - Python vulnerability
4. USN-5928-1 - systemd vulnerabilities
5. USN-5767-3 - Python vulnerability
6. USN-5921-1 - rsync vulnerabilities (AWS)
7. USN-5917-1 - Linux kernel vulnerabilities
8. USN-5871-2 - Git regression (AWS)
9. USN-5900-1 - tar vulnerability
10. USN-5891-1 - curl vulnerabilities

Questions? Contact us

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

STEPS TO APPLY THE UPDATE

1. Download the GreenRADIUS update v4.5.9.9 zip file
   (md5 = 168cf88c933a7470a160ad3088d68a4f, sha256 = 138feff0d07b47e41c964c3896115baf757813119261b1ed09c62758919d206a)
   Extract it, and it will result in a folder "GreenRADIUS_4599_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_4599_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_4599_Update

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v4.5.8.8

1. Fixed an issue in the Token Assignment report in which no records were displayed in the report when Mobile app tokens were present (assigned) on the server and "Mobile" token type was selected as a filter for generating the report.
2. Fixed an issue in the LDAP Authenticator Module where authentications failed for users with special characters in the username.