RELEASE NOTES

GreenRADIUS UPDATE v4.1.8.8

RELEASE DATE
MAY 20, 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 v4.1.8.8 zip file (md5 = 80b79fcaff65ac191facc32eb402e01e). Extract it, and it will result in a folder "GreenRADIUS_4188_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_4188_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_4188_Update

UBUNTU VULNERABILITIES PATCHED

1. USN-4360-1 - json-c vulnerability
2. USN-4359-1 - APT vulnerability
3. USN-4357-1 - IPRoute vulnerability
4. USN-3911-2 - file regression
5. USN-4342-1 - Linux kernel vulnerabilities
6. USN-4333-1 - Python vulnerabilities
7. USN-4319-1 - Linux kernel vulnerabilities
8. USN-4324-1 - Linux kernel vulnerabilities
9. USN-4313-1 - Linux kernel vulnerability
10. USN-4302-1 - Linux kernel vulnerabilities
11. USN-4300-1 - Linux kernel vulnerabilities
12. USN-4309-1 - Vim vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v4.1.6.7

1. Lockout mechanism implemented in the two-factor authentication API (disabled by default)
2. New management API to delete tokens
3. Input parameter validations are added in the management APIs
4. License checking enhancement in the authentication process
5. Fixed error message issue in the Windows agent Test and Save buttons
6. Support for log rotation of a few log files
7. Returning of the timestamp and lockout status is added in the authentication API response
8. Time zone change is made uniform across all the containers that generate logs
9. Network timeout is added while establishing the LDAP connection during authentication attempts

Questions? Contact us

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