RELEASE NOTES

GreenRADIUS UPDATE v6.1.4.4

RELEASE DATE

JULY 31, 2025

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v6.1.1.1 or later.
b. A minimum of 4GB RAM is recommended for this update to be applied successfully.
c. Before applying updates, we highly 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. Processing of authentication requests may be affected for some time during this process.

STEPS TO APPLY THE UPDATE

1. Download the GreenRADIUS update v6.1.4.4 zip file
   (md5 = 7c25eb3241443f4786095f254a538030, sha256 = 22070ed9a36410b78448e2b35c0247e7b59a15f0c2d0b0f9840e4647b7050b35)
   Extract it, and it will result in a folder "GreenRADIUS_6144_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_6144_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_6144_Update

VULNERABILITIES PATCHED

1. USN-7651-1 - Linux kernel vulnerabilities
2. USN-7635-1 - GnuTLS vulnerabilities
3. USN-7634-1 - GNU C Library vulnerabilities
4. USN-7412-2 - GnuPG regression
5. USN-7619-1 - libssh vulnerabilities
6. USN-7609-1 - Linux kernel vulnerabilities
7. USN-7604-1 - Sudo vulnerabilities
8. USN-7599-1 - urllib3 vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.3.3

1. Removed the provision to switch back to the old LDAP Authenticator Module once the new LDAP Authenticator Module is enabled
2. A proper error message is now displayed when authentication fails on the self-service portal due to an invalid or expired certificate

Questions? Contact us

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