

RELEASE NOTES
GreenRADIUS UPDATE
v6.1.9.9

RELEASE DATE
DECEMBER 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.

VULNERABILITIES PATCHED

1. USN-7931-1 - Linux kernel vulnerabilities
2. USN-7929-1 - usbmuxd vulnerability
3. USN-7927-1 - urllib3 vulnerabilities
4. USN-7924-1 - libpng vulnerabilities
5. USN-7919-1 - GNU binutils vulnerabilities
6. USN-7916-1 - python-apt vulnerability
7. USN-7899-1 - GNU binutils vulnerabilities

STEPS TO APPLY THE UPDATE

1. Download the [GreenRADIUS update v6.1.9.9 zip file](#)
(md5 = 084434f1553ef2e55d8c06a75fa9df09, sha256 = d9c79e29ac821a130832e0dbaec8548ce76ee4b22d561dd95e91fc06dce217bc)
Extract it, and it will result in a folder
"GreenRADIUS_6199_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_6199_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_6199_Update



ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.8.8

1. Added support configuring IPv6 in the GreenRADIUS network configuration script

Questions? Contact us

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