

GreenRADIUS UPDATE

v6.1.14.14

RELEASE DATE
MAY 29, 2026



GreenRocket
Security

NOTES

- This GreenRADIUS update can only be applied to v6.1.1.1 or later.
- A minimum of 4GB RAM is recommended for this update to be applied successfully.
- Before applying updates, we highly recommend creating a snapshot of the GreenRADIUS VM in your virtualization server environment that can act as a backup.
- 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

- Download the [GreenRADIUS update v6.1.14.14 zip file](#)
(md5 = 48a2af6d62dd96820164825d4bd1f49c, sha256 = 85c3de35ced98842727c97a042449e42a5043132670e4aed1c457dbdc631f608)
Extract it, and it will result in a folder "GreenRADIUS_611414_Update"
- Copy this folder onto the GreenRADIUS host in /home/gradmin using a client like scp or WinSCP
- Log in to GreenRADIUS over ssh
- Run the following commands:
 - \$ cd /home/gradmin/GreenRADIUS_611414_Update
 - \$ sudo chmod +x install_update.sh
 - \$ sudo sh install_update.sh
- 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.
- After a successful update, it is recommended to clean up the new directory created for this update process.
 - \$ sudo rm -rf /home/gradmin/GreenRADIUS_611414_Update



VULNERABILITIES PATCHED

- USN-8293-1 - Bind vulnerabilities (AWS)
- USN-8284-1 - GnuTLS vulnerabilities
- USN-8283-1 - rsync vulnerabilities (AWS)
- USN-8278-1 - Linux kernel vulnerabilities
- USN-8246-1 - Vim vulnerabilities
- USN-8254-1 - Linux kernel vulnerabilities
- USN-8253-1 - Postfix vulnerability
- USN-8251-1 - libpng vulnerabilities
- USN-8249-1 - dpkg vulnerability
- USN-8233-1 - nghttp2 vulnerability
- USN-8229-1 - sed vulnerability
- USN-8227-1 - curl vulnerabilities
- USN-8226-1 - kmod update
- USN-8222-1 - OpenSSH vulnerabilities
- USN-8213-1 - Vim vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.13.13

- Added support to configure the "Prompt For OTP" OTP input method and its associated prompt text by RADIUS client instead of globally

Questions? Contact us

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