

RELEASE NOTES
GreenRADIUS UPDATE
v6.1.7.7

RELEASE DATE
OCTOBER 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-7836-1 - Bind vulnerabilities (AWS)
2. USN-7835-1 - Linux kernel vulnerabilities
3. USN-7824-1 - Redis vulnerability
4. USN-7792-1 - Linux kernel vulnerabilities
5. USN-7786-1 - OpenSSL vulnerabilities
6. USN-7785-1 - Open VM Tools vulnerability



STEPS TO APPLY THE UPDATE

1. Download the [GreenRADIUS update v6.1.7.7 zip file](#)
(md5 = 359de8e8afa89a93fadd9faeca15eaa9, sha256 = 667e2f8033d180f4dcabad7a33db430a37e5fe75c97733e4406e715ea5879bc0)
Extract it, and it will result in a folder
"GreenRADIUS_6177_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_6177_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_6177_Update

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.6.6

1. GreenRADIUS now provides broader support for OATH tokens (HOTP and TOTP) from any manufacturer by eliminating vendor-specific constraints

Questions? Contact us

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