RELEASE NOTES

GreenRADIUS UPDATE v6.1.15.15

RELEASE DATE

JUNE 30, 2026

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 v6.1.15.15 zip file
   (md5 = 08bbec799bfea31debaba302f0f207c8, sha256 = 1c2f97e50efa6c944c76d5788f223bb0a016a24d520e4ca9cd001f410b652901)
   Extract it, and it will result in a folder "GreenRADIUS_611515_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_611515_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_611515_Update

VULNERABILITIES PATCHED

1. USN-8480-1 - SQLite vulnerabilities
2. USN-8477-1 - tar vulnerability
3. USN-8475-1 - AMD Microcode vulnerabilities (AWS)
4. USN-8456-1 - libxml2 vulnerability
5. USN-8451-1 - Vim vulnerabilities
6. USN-8415-1 - Vim vulnerabilities
7. USN-8414-1 - OpenSSL vulnerabilities
8. USN-8349-2 - rsync regression (AWS)
9. USN-8402-1 - systemd vulnerabilities
10. USN-8379-1 - urllib3 vulnerabilities
11. USN-8373-1 - Linux kernel vulnerabilities
12. USN-8362-1 - XZ Utils vulnerability
13. USN-8319-1 - Libgcrypt vulnerabilities
14. USN-8304-1 - Vim vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.14.14

1. User PIN enhancements:
   a) Added the ability to force users to change their PIN when a temporary PIN is issued by an admin
   b) Added support for configurable PIN expiration, where PINs expire after a configured number of days
2. Enhanced GreenRADIUS containerized deployments by removing dependencies on host-level services

Questions? Contact us

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