RELEASE NOTES

GreenRADIUS UPDATE v5.2.16.16

RELEASE DATE

FEBRUARY 28, 2025

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v5.2.12.12 or later.
b. A minimum of 4GB RAM is recommended for this update to be applied successfully.
c. Before applying updates, we 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, and processing of authentication requests may be affected for some time during this process.

STEPS TO APPLY THE UPDATE

1. Download the GreenRADIUS update v5.2.16.16 zip file
   (md5 = bc410ee77486a76bb7e41bf5e3907e3a, sha256 = 440680af12cf0e2150063ad513a85f0a0d4fc622dd4c56d1f0d7455f7d2f640a)
   Extract it, and it will result in a folder "GreenRADIUS_521616_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_521616_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_521616_Update

VULNERABILITIES PATCHED

1. USN-7220-1 - Vim vulnerability
2. USN-7236-1 - Linux kernel vulnerabilities
3. USN-7240-1 - libxml2 vulnerabilities
4. USN-7241-1 - Bind vulnerabilities (AWS)
5. USN-7244-1 - Jinja2 vulnerabilities
6. USN-7257-1 - Kerberos vulnerability
7. USN-7259-1 - GNU C Library vulnerability
8. USN-7261-1 - Vim vulnerability
9. USN-7269-1 - Intel Microcode vulnerabilities
10. USN-7270-1 - OpenSSH vulnerabilities
11. USN-7275-1 - Libtasn1 vulnerability
12. USN-7278-1 - OpenSSL vulnerabilities
13. USN-7280-1 - Python vulnerability
14. USN-7281-1 - GnuTLS vulnerability

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v5.2.15.15

1. Added support to configure group membership, VSA, and group prioritization settings per each RADIUS client (rather than at the domain level). **NOTE: All RADIUS client, group membership, VSA, and group prioritization settings have been moved to the Global Configuration tab > Client-based Authentication Policies page**
2. The Token Assignment Management API now indicates whether users are present in the user import from the directory server or not

Questions? Contact us

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