RELEASE NOTES

GreenRADIUS HOTFIX v5.2.8.8-2

RELEASE DATE

JULY 15, 2024

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v5.2.8.8.
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.

VULNERABILITIES PATCHED

1. USN-6859-1 - OpenSSH vulnerability (CVE 2024-6387)
2. USN-6852-1 - Wget vulnerability
3. USN-6851-1 - Netplan vulnerabilities
4. USN-6854-1 - OpenSSL vulnerability
5. USN-6851-2 - Netplan regression

STEPS TO APPLY THE UPDATE

1. Download the GreenRADIUS hotfix v5.2.8.8-2 zip file
   (md5 = af1f3346a526a935781d1ae172491476, sha256 = fdc5e785b8582ac5175b71d3af05a7e57d1bee557ddec8e3f955021d670e594e)
   Extract it, and it will result in a folder "GreenRADIUS_5288-2_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_5288-2_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_5288-2_Update

Questions? Contact us

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