RELEASE NOTES

GreenRADIUS UPDATE v5.2.9.9

RELEASE DATE

JULY 31, 2024

GreenRocket Security

NOTES

a. This GreenRADIUS update can only be applied to v5.1.1.1 or later.
b. A minimum of 4GB RAM is recommended for this update to be applied successfully.
c. Before applying updates, we 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 v5.2.9.9 zip file
   (md5 = 1fef05d5a6b9d4f00e411e7316af3687, sha256 = e4c1f6e2ec791a3da206e3615530c03771aaf3f7f61ab2290c83040154f756be)
   Extract it, and it will result in a folder "GreenRADIUS_5299_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_5299_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_5299_Update

VULNERABILITIES PATCHED

1. USN-6852-1 - Wget vulnerability
2. USN-6851-1 - Netplan vulnerabilities
3. USN-6854-1 - OpenSSL vulnerability
4. USN-6851-2 - Netplan regression
5. USN-6859-1 - OpenSSH vulnerability (CVE 2024-6387)
6. USN-6872-1 - Linux kernel vulnerabilities
7. USN-6873-1 - Linux kernel vulnerabilities (AWS)
8. USN-6891-1 - Python vulnerabilities
9. USN-6900-1 - Linux kernel vulnerabilities
10. USN-6895-3 - Linux kernel vulnerabilities (AWS)
11. USN-6906-1 - python-zipp vulnerability

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v5.2.8.8

1. Added a configuration option to RADIUS clients to enable enforcement of the "Message-Authenticator" client attribute to mitigate the "BlastRADIUS" vulnerability
2. Fixed a regression that caused issues when configuring the LDAP Authenticator Module
3. Fixed an issue in the Token Assignment Management API where requests failed if GreenRADIUS had inactive users with Latin characters in their usernames
4. Minor bug fixes in GreenRADIUS reports

Questions? Contact us

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