RELEASE NOTES

GreenRADIUS UPDATE v7.1.1

RELEASE DATE

OCTOBER 31, 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 **more time than a usual update, about 15 to 30 minutes**. Processing of authentication requests may be affected for some time during this process.

STEPS TO APPLY THE UPDATE

1. Download the GreenRADIUS update v7.1.1 zip file
   (md5 = c0a0df283d1fc44496c87dc5f9d92296, sha256 = 6671fc0da032826ab2bb3a8898aa5bd20bff16ab445f18be969d215baf3967be)
   Extract it, and it will result in a folder "GreenRADIUS_711_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_711_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_711_Update

VULNERABILITIES PATCHED

1. USN-8956-1 - Brotli vulnerability
2. USN-8954-1 - zlib vulnerability
3. USN-8948-1 - PHP vulnerabilities
4. USN-8945-1 - XZ Utils vulnerability
5. USN-8944-1 - ca-certificates update
6. USN-8934-1 - PyJWT vulnerabilities
7. USN-8929-1 - Bind vulnerabilities (AWS)
8. USN-8928-1 - OpenSSH vulnerabilities
9. USN-8927-1 - curl vulnerabilities
10. USN-8926-1 - urllib3 vulnerabilities
11. USN-8916-1 - PyJWT vulnerabilities
12. USN-8913-1 - libx11 vulnerabilities
13. USN-8910-1 - libxml2 vulnerabilities
14. USN-8895-1 - Sudo vulnerability
15. USN-8887-1 - Linux kernel vulnerabilities
16. USN-8881-1 - FreeType vulnerability
17. USN-8874-1 - sg3_utils vulnerability
18. USN-8861-1 - OpenSSL vulnerabilities
19. USN-8847-1 - OpenSSL vulnerabilities

ENHANCEMENTS, NEW FEATURES, AND BUG FIXES OVER GreenRADIUS v6.1.18.18

1. Added a Management API to unassign mobile push app tokens
2. Added a mitigation for CVE-2026-115560

Questions? Contact us

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