

RELEASE NOTES  
**GreenRADIUS HOTFIX**  
**v6.1.18.18-1**

RELEASE DATE  
**OCTOBER 23, 2026**



## NOTES

- This GreenRADIUS hotfix can only be applied to v6.1.18.18.
- A minimum of 4GB RAM is recommended for this update to be applied successfully.
- Before applying updates, we highly recommend creating a snapshot of the GreenRADIUS VM in your virtualization server environment that can act as a backup.
- The update process may take about 10 to 15 minutes. Processing of authentication requests may be affected for some time during this process.

## VULNERABILITIES PATCHED

- CVE-2026-109618 - Php2shell (PHP vulnerabilities)
- CVE-2026-109619 - Php2shell (PHP vulnerabilities)
- CVE-2026-111497 - Node2Shell (Node.js Brotli vulnerability)
- USN-8954-1 - zlib vulnerability
- USN-8945-1 - XZ Utils vulnerability
- USN-8944-1 - ca-certificates update
- USN-8934-1 - PyJWT vulnerabilities
- USN-8932-1 - curl vulnerabilities
- USN-8929-1 - Bind vulnerabilities
- USN-8928-1 - OpenSSH vulnerabilities
- USN-8926-1 - urllib3 vulnerabilities
- USN-8917-1 - Linux kernel vulnerabilities
- USN-8916-1 - PyJWT vulnerabilities
- USN-8913-1 - libx11 vulnerabilities
- USN-8910-1 - libxml2 vulnerabilities
- USN-8903-1 - Linux kernel vulnerabilities
- USN-8895-1 - Sudo vulnerability
- USN-8881-1 - FreeType vulnerability
- USN-8874-1 - sg3\_utils vulnerability
- USN-8817-3 - Linux kernel (AWS) vulnerabilities
- USN-8847-1 - OpenSSL vulnerabilities
- USN-8840-1 - libevent vulnerabilities



## STEPS TO APPLY THE UPDATE

- Download the [GreenRADIUS hotfix v6.1.18.18-1 zip file](#)  
(md5 = 6d37d6e49373d32a19b682c296bf3446, sha256 = 5c0bb2ce5739ed4b61d11e1ec5e5b19991c71d5b0a70b19b1b7215a7f65d82f6)  
Extract it, and it will result in a folder  
"GreenRADIUS\_611818-1\_Update"
- Copy this folder onto the GreenRADIUS host in  
/home/gradmin using a client like scp or WinSCP
- Log in to GreenRADIUS over ssh
- Run the following commands:
  - \$ cd /home/gradmin/GreenRADIUS\_611818-1\_Update
  - \$ sudo chmod +x install\_update.sh
  - \$ sudo sh install\_update.sh
- 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.
- After a successful update, it is recommended to clean up the new directory created for this update process.
  - \$ sudo rm -rf  
/home/gradmin/GreenRADIUS\_611818-1\_Update

## Questions? Contact us

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