درس ۴ از ۱۲

Rocky Linux 9 & 10

Install · Migrate · Differences

آپدیت‌ها، Errata و امنیت در Rocky Linux

دوره کامل · Rocky Linux 10.3 & 9.9 (Nov 2026)



در درس چهارم چه یاد می‌گیرید

- اصلاحات امنیتی چگونه جریان می‌یابند: Rocky ← RHEL
- Rocky Errata (RLSA، RLBA، RLEA) و dnf updateinfo
- بررسی یک CVE روی سیستم شما
- آپدیت خودکار با dnf-automatic
- آپدیت کِرنِل، ریبوت و برگشت
- مستحکم‌سازی Rocky: SELinux، firewalld، crypto policies، OpenSCAP
- نظارت بر سرورها بدون اشتراک

اصلاحات امنیتی چگونه به Rocky می‌رسند

قدم	چه اتفاق می‌افتد
۱	یک آسیب‌پذیری (CVE) پیدا و در upstream اصلاح می‌شود
۲	Red Hat یک هشدار (RHSA) و بسته‌های آپدیت‌شده RHEL منتشر می‌کند
۳	منابع اصلاح‌شده عمومی ظاهر می‌شوند (CentOS Stream و منابع عمومی دیگر)
۴	Rocky بسته‌ها را دوباره می‌سازد، آزمایش و امضا می‌کند
۵	Rocky یک هشدار (RLSA) منتشر می‌کند و بسته‌ها به آینه‌ها می‌رسند
تأخیر عادی	معمولاً چند ساعت تا چند روز؛ اصلاحات فوری اولویت دارند

Rocky Errata

نوع	معنی	مثال
RLSA	هشدار امنیتی Rocky Linux	RLSA-2026:xxxx openssl
RLBA	هشدار اصلاح باگ	RLBA-2026:xxxx systemd
RLEA	هشدار بهبود	RLEA-2026:xxxx podman
شدت	Critical، Important، Moderate، Low	اول Critical و Important را patch کنید
کجا	errata.rockylinux.org؛ همچنین داخل dnf	جستجو بر اساس CVE یا بسته

dnf updateinfo با Errata

```
[student@rocky1 ~]$ dnf updateinfo summary
Updates Information Summary: available
    3 Security notice(s)
        1 Important Security notice(s)
        2 Moderate Security notice(s)
    5 Bugfix notice(s)
[student@rocky1 ~]$ dnf updateinfo list --security
[student@rocky1 ~]$ dnf updateinfo info RLSA-2026:xxxx
[student@rocky1 ~]$ sudo dnf upgrade --security                # security fixes only
[student@rocky1 ~]$ sudo dnf upgrade --advisory=RLSA-2026:xxxx # one advisory
[student@rocky1 ~]$ sudo dnf upgrade --sec-severity=Critical
```

آیا این CVE روی سرور من اصلاح شده است؟

```
[student@rocky1 ~]$ dnf updateinfo list --cve CVE-2026-xxxxx      # waiting?
[student@rocky1 ~]$ dnf updateinfo list --installed --cve CVE-2026-xxxxx   # already fixed?
[student@rocky1 ~]$ rpm -q --changelog openssl | grep -i CVE-2026 | head
[student@rocky1 ~]$ rpm -q openssl kernel
[student@rocky1 ~]$ uname -r                # the RUNNING kernel may be older!
[student@rocky1 ~]$ sudo dnf needs-restarting -r
Core libraries or services have been updated since boot-up:
  * kernel
Reboot is required to fully utilize these updates.
```

آپدیت خودکار با dnf-automatic

```
[student@rocky1 ~]$ sudo dnf install -y dnf-automatic
[student@rocky1 ~]$ sudo vim /etc/dnf/automatic.conf
[commands]
upgrade_type = security          # or default (all updates)
apply_updates = yes
reboot = when-needed             # check: man dnf-automatic
[emitters]
emit_via = motd                  # or email, command_email
[student@rocky1 ~]$ sudo systemctl enable --now dnf-automatic.timer
[student@rocky1 ~]$ systemctl list-timers dnf-automatic*
```

آپدیت کِرنِل، ریبوت و برگشت

چگونه	کار
installonly_limit=3 در /etc/dnf/dnf.conf (پیش‌فرض)	کِرنِل‌های قدیمی را نگه دارید
اگر نو ناکام شد، آن را در منوی GRUB انتخاب کنید	بوت با کِرنِل قدیمی‌تر
sudo grubby --set-default /boot/vmlinuz-<version>	آن را پیش‌فرض کنید
sudo grubby --info=ALL | grep ^kernel	دیدن کِرنِل‌ها
توسط Rocky ارائه نمی‌شود؛ گزینه‌های تجاری وجود دارد (مثلاً از CIQ)	Live patching
snapshot قبل از تغییرات بزرگ؛ <dnf history undo <id	برگرداندن بسته‌ها

مستحکم‌سازی Rocky با ابزارهای رایگان

```
[student@rocky1 ~]$ getenforce                          # Enforcing — keep it!
[student@rocky1 ~]$ sudo firewall-cmd --list-all
[student@rocky1 ~]$ update-crypto-policies --show       # DEFAULT
[student@rocky1 ~]$ sudo dnf install -y openscap-scanner scap-security-guide
[student@rocky1 ~]$ ls /usr/share/xml/scap/ssg/content/ | grep -i -E 'rl|rocky|rhel'
[student@rocky1 ~]$ sudo oscap xccdf eval --profile cis --report /tmp/cis.html \
      /usr/share/xml/scap/ssg/content/<datastream-for-your-version>.xml
[student@rocky1 ~]$ sudo dnf install -y fail2ban aide ; sudo systemctl enable --now fail2ban
```

نظارت بر سرورها بدون اشتراک

گزینه رایگان	نیاز
dnf updateinfo summary از راه Ansible یا یک گزارش cron	آپدیت‌های منتظر
Cockpit، PCP، Prometheus node_exporter + Grafana	سلامت و معیارها
rsyslog مرکزی یا journald remote؛ Loki یا OpenSearch	لاگ‌ها
OpenSCAP؛ اسکنرهای متن باز مانند Trivy برای image ها	اسکن آسیب‌پذیری
Foreman/Katello (درس ۱۱)، Ansible	فهرست و patch
CIQ و دیگران پشتیبانی و مدیریت برای Rocky ارائه می‌کنند	تجاری

خلاصه و کارخانگی

- اصلاحات از RHEL ← منابع عمومی ← بازسازی RLSA ← Rocky جریان می‌یابند
- dnf updateinfo summary / list --security / --cve
- dnf upgrade --security؛ dnf-automatic برای خودکارسازی
- ریبوت برای اصلاحات کِرنِل: needs-restarting -r؛ grubby برای برگشت
- مستحکم‌سازی رایگان: SELinux، firewalld، crypto policies، OpenSCAP، fail2ban
- کارخانگی: هشدارهای امنیتی منتظر را روی rocky1 گزارش دهید؛ dnf-automatic را برای آپدیت امنیتی فعال کنید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید