2nd Annual
MidPoint Community Meetup

MidPoint Docker Images: Vulnerability and Patch Management

Evolveum

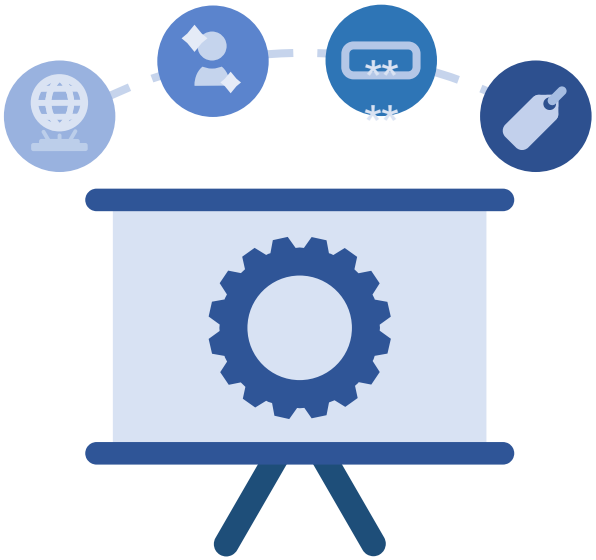
Martin Špánik, May 2026
CISO & Compliance

Agenda

- Actual state
- Patch management process
- New naming convention of Docker images
- Use cases for deployment
- New risks
- Vulnerability reporting in AI era

Actual state

- Docker images released with midPoint releases
  - New relases each 3 months
- Static images no changes after release
  - OS layer
  - MidPoint layer
- Need to patch faster
  - Split patch management of OS layer and midPoint



Patch management process – 1/2

- Identification of vulnerabilities
  - External or internal information (security report, code analysis)
  - Internal automated scanning: OWASPs Dependency Track
- Initial triage
  - MidPoint layer – analysis and scheduling
  - Docker image OS layer – prioritization and patch processing
- Patch management - midPoint
  - Scheduling – next maintenance release, security release

Patch management process – 2/2

- Patch management - docker image
  - Must be patched in underlying OS
  - New docker image: OS updated, midPoint untouched
    - Updated OS layer
    - Latest release of midPoint
    - The same image tag reused for new content
  - Supported releases and docker images
- False positives and accepted vulnerabilities
  - Some reports reporting false positives
    - Eventually – all Critical and High are remediated

New naming convention of docker images

- Floating tags
- Stable releases
  - Release tag: 4.11.3-alpine
  - Minor version tag: 4.11-alpine-latest
    - current maintenance release of 4.11
  - Latest tag: latest / alpine-latest
    - latest maintenance release
- Unstable releases
  - Master branch: alpine-nightly
  - Support branch: 4.10-alpine-nightly
- Supported OS: alpine, ubuntu, rockylinux
- Maintenance ID in all versions - 4.11.0 release

Use Cases: Deployment of midPoint Containers

Stable releases		
Current midPoint, with current OS	**evolveum/midpoint:4.11-alpine-latest**	Production env.
Fixed midPoint, current OS	**evolveum/midpoint:4.11.3-alpine**	Prod with experimental features
Fixed midPoint, fixed OS	**evolveum/midpoint@sha256:DIGEST**	Full control over changes. Manual updates.
Unstable releases		
Actual support branch	**evolveum/midpoint:4.11-alpine-nightly**	
Master branch	**evolveum/midpoint:alpine-nightly**	

- Tag ":latest"
  - For evaluation only! MidPoint requires manual upgrades to new minor version (to 4.11, 4....)

New Risks

- Faster enough? / Not too fast?
  - Supply chain attacks...
- Operation / availability issues
  - OS layer updates – lower risk, docker images are tested.
  - MidPoint layer updates – automated updates
- Do not use `latest` tag in production

Update schedule

- Nightly builds already deployed in Docker-hub
- Stable builds starts with next maintenance release
  - 25,26 May 2026
  - 4.10.3, 4.9.7, 4.8.12
- Actual docker images are unchanged
- Communication over mailing list

Vulnerability reporting in AI era

- Still reporting to security@evolveum.com
- NO information in support portal
- Release notes, security advisories

- AI generated reports – need help
- Put human in the loop – please analyze reports, provide PoCs and test them
  - Insert your knowledge of midPoint

Conclusion

- Patched versions of docker images
- 2 layers of patching:
  - OS layer – automatic and fast
  - MidPoint – more complex – midPoint release
- Floating tags of docker images
- Actual images unchanged
- Security release of midPoint may come
- Responsible reporting


Evolveum
Thank you for your attention
Feel free to ask your questions now!
Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
2nd Annual
MidPoint Community Meetup