



adaptTo()

EUROPE'S LEADING AEM DEVELOPER CONFERENCE
28th – 30th SEPTEMBER 2026

Securing AEM Customer Code

Andrés Bott & Ramon Bißwanger, Adobe



Andrés Bott

Sr. Computer Scientist (Adobe)



Ramon Bißwanger

Sr. Computer Scientist (Adobe)

Agenda

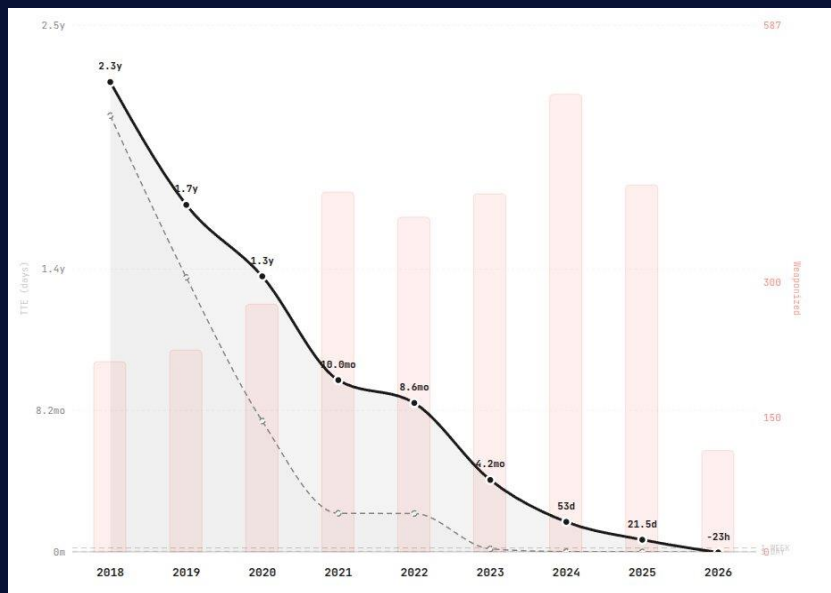
- current landscape
- Automated vulnerability fixes
 - Identify
 - Fix with Sites Optimize
 - Fix with MCP (Claude Code)
- Prevention with Renovate
 - Practical use-cases

Automated vulnerability fixes

Security: AI landscape

Vulnerabilities identified and exploited faster than ever

- 2018: ~ 2.3 years
- 2026: hours



<https://zerodayclock.com>

AEM Security: Focus on customer code

Features with focus on customer code / config

- Vulnerabilities in 3rd party libraries
 - OWASP 2021: A06: Vulnerable and Outdated Components
 - OWASP 2025: A03: Software Supply Chain Failures
- More to come:
 - Focus on OWASP top 10
 - permissions, OSGI configs, etc..

The setup: Super Cool Bundle


super-cool-bundle
Public

Watch 0
Fork 0
Star 0

main
1 Branch
2 Tags

Code

 andresbott	fix: upgrade snakeyaml to 2.4 to resolve CVE-2022-1471 (#1) ✓	60200c4 · 2 weeks ago	4 Commits
 .github/workflows	build: add maven Makefile and tag-triggered release wor...		2 weeks ago
 src/main/java/com/github/andresbott/super...	fix: upgrade snakeyaml to 2.4 to resolve CVE-2022-1471 (...)		2 weeks ago
 .gitignore	feat: add deliberately-vulnerable OSGi bundle embedding...		2 weeks ago
 Makefile	build: add maven Makefile and tag-triggered release wor...		2 weeks ago
 README.md	fix: upgrade snakeyaml to 2.4 to resolve CVE-2022-1471 (...)		2 weeks ago
 jitpack.yml	build: add maven Makefile and tag-triggered release wor...		2 weeks ago
 pom.xml	fix: upgrade snakeyaml to 2.4 to resolve CVE-2022-1471 (...)		2 weeks ago


README

super-cool-bundle

Showcase bundle for **adaptTo() 2026** — a tiny OSGi bundle used to demonstrate *transitive* dependency detection in SBOM / security scanning.

Version 2.0.0 is the remediated release. It depends on — and embeds as a nested lib — a **non-vulnerable** release of SnakeYAML (`org.yaml:snakeyaml:2.4`), which fixes [CVE-2022-1471](#). Anything that depends on this bundle now inherits a clean dependency transitively, and a byte-level scanner finds `snakeyaml-2.4.jar` inside the bundle (`Bundle-ClassPath: .,snakeyaml-2.4.jar`) — so an SBOM / security scan comes back clean.

About

showcase bundle for adaptto 2026

-  Readme
-  Activity
-  0 stars
-  0 watching
-  0 forks

Report repository

Releases 2

 **2.0.0** Latest
2 weeks ago

[+ 1 release](#)

Packages

No packages published

Contributors 1

 **andresbott** Andres Bott

Languages



-  Makefile 70.6%
-  Java 29.4%

- Identify: Continuous scanning

- SBOM of deployed AEM code:
 - Includes transitive and embedded dependencies
- AEM specific:
 - Understands content packages
- Daily verifications
- At scale: identify top issues in AEMCS
 - e.g. vulnerable component on ~20% of customers

2. Discover : Experience hub (demo)


The tiger and the crane: bott-adapto-2026

Home
Universal Editor
Cloud Manager
Cloud Acceleration Manager
Software Distribution
Extension Manager
Enterprise Context

Security and Compliance

 Security Health
Penetration Tests
Customer Managed Keys
Advanced WAF
CDN Traffic
Security Documents

Tools

Security Health

7
Vulnerabilities
↓ 65 (30 days)

0
Unnecessary Permissions
↓ 2 (30 days)

Environment
cm-p15854-e2240987 (Development)



1 third-party library in your application code has known vulnerabilities

Last scan: 23/09/2026
Development
cm-p15854-e2240987 (bott-adapto-2026)

Vulnerabilities

7
Vulnerabilities

Details

Improve your security health in Sites Optimizer
Enhance your website's security and performance while reducing maintenance and update costs.
More about Sites Optimizer

Let's fix a it: ASO

3. Fix: AEM Sites Optimizer (1)

- Northstar:
 - automatic fixes deployed with minimal human integration
- Security Opportunities
 - Focus on security aspect of project
 - Seamless integration

3. Fix: AEM Sites Optimizer (2)

- AI based code patches
- Fixes customer code
- Intrinsic AEM knowledge
- Open Pull request on source

3. Fix: AEM Sites Optimizer (demo)

Adobe Experience Manager Sites Optimizer

Overrides on

Sites Internal

Get Support

Good evening, Andres!

Explore publish-p15854-e2240987.adobeamcloud.com's growth journey, track improvements, and see how optimizations are making a real impact.

publish-p15854-e2240987.adobeamcloud.com

WKND Adventures and Travel

0

Opportunities optimized

1

Opportunities pending

Pageviews

NA

Avg. Engagement

NA

Site Speed

NA

Highest impact opportunities

All

Traffic acquisition

Engagement and conversion

Web performance

Security

Compliance and accessibility

Filter by URL

Showing 1 optimization opportunity

Only show starred

Sort by Recently added

Third-Party Libraries - security risks detected

Last updated 21 Sept 2026

3rd Party Libraries

Security

7

Vulnerabilities

Star

Skip

Review

Let's list and fix a it: MCP

4. Fix: AEM MCP

- AEM MCP server
 - Get security details into agent context
 - Login as user => same access as developer
- local harness
 - Your skills, tools, access and project context
 - e.g. full hands off with local skill and AEM coordinates

Claude Code (demo)

```
Claude Code v2.1.283
Opus 5.5 (Bedrock) with xhigh effort · Amazon Bedrock
~/..datos/edit/programacion/adaptto26/wknd-adaptto-2026

● agents-md: no CLAUDE.md found; AGENTS.md loaded:
/home/bott/..datos/edit/programacion/adaptto26/wknd-adaptto-2026/AGENTS.md

> can you show me the security posture of my environment █

[Opus 5.5 (Bedrock)] █ wknd-adaptto-2026 | 🌱 auto-fix | █ 0% 0/200k | $0.00 | ⌚ 5s
>> auto mode on (shift+tab to cycle) · PR #16
```

4. Fix: AEM MCP (2)

- Skill in repository
 - Identify the applicable environment
 - Pull security information
 - Instructions on how to fix
 - Validate and open a PR
- Agents.md:
 - Cloud Manager coordinates

Stay ahead: an automated Renovate pipeline

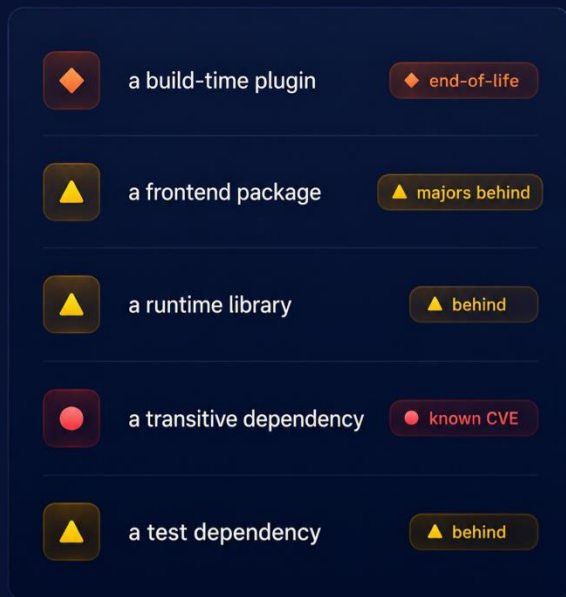
“The time to repair the roof is when the sun is shining.”
- **John F. Kennedy**

The problem

- Main effort: version jump when addressing vulnerabilities



The complexity



- Too many dependencies to manage them by hand
- AEM archetype (end July 2026)
 - 150+ maven + 550+ npm dependencies (incl. transitive)

Renovate – open-source dependency automation



Open source



Works everywhere



Config as code



Security-aware

Using Renovate with AEM as a Cloud Service

The idea: automation



AEM BYOG repositories + Renovate

- Recommendation: BYOG git repositories
 - Hosted renovate with scheduled scans
 - Github Actions for automated validation
- Setup effort
 - Define Renovate configuration (grouping, auto-merge, exclusions, ...)
 - Sample: <https://github.com/bisswanger/aem-byog-renovate>

Open
Dependency Dashboard #6

Open

The following updates have all been created. To force a retry/rebase of any, click on a checkbox below.

- ☐ [Update dependency webpack-dev-server from 4.11.1 to 5.2.6 \[SECURITY\]](#) ...
- ☐ [Update AEM Core Components from 2.28.0 to 2.32.4](#) (com.adobe.cq:core.wcm.components.testing.aem-mock-plugin, com.adobe.cq:core.wcm.components.core) ...
- ☐ [Update dependency aem-clientlib-generator from 1.8.0 to 1.10.0](#) ...
- ☒ [Update dependency io.wcm:io.wcm.testing.aem-mock-junit5 from 5.5.4 to 5.7.4](#) ...
- ☐ [Update dependency org.apache.sling:org.apache.sling.models.impl from 1.4.14 to 1.7.8](#) ...
- ☐ [Update dependency sass from 1.54.9 to 1.102.0](#) ...
- ☐ [Update dependency typescript from 4.8.3 to 4.9.5](#) ...
- ☐ [Update dependency uk.org.lidalia:slf4j-test from 1.0.1 to 1.2.0](#) ...
- ☐ [Update ESLint](#) (@typescript-eslint/eslint-plugin, @typescript-eslint/parser, eslint, eslint-webpack-plugin) ...
- ☐ [Update mockito monorepo from 4.1.0 to 4.11.0](#) (org.mockito:mockito-junit-jupiter, org.mockito:mockito-core) ...

← Renovate branch validation

✓ Update npm dev dependencies - fixes #47

Summary

All jobs

mvn clean verify
Cloud Manager pipeline run

Run details

Usage

Workflow file

Triggered via pull request 3 days ago	Status	Total duration	Artifacts
renovate[bot] synchronize #16 renovate/npm-dev-dependen...	Success	37m 34s	—

renovate-validation.yml

on: pull_request

✓ mvn clean verify
46s

✓ Cloud Manager pipeli...
36m 42s

AEM CM repositories + Renovate

- Using standard Cloud Manager repository
 - Does not support PRs / running renovate
 - Approach:
 - Run renovate locally (check / branches / validation)
 - Uses Gitea as a local temporary repository host
- Demo implementation
 - <https://github.com/bisswanger/aem-cm-renovate>

AEM CM repositories + Renovate



Renovate report — Ramon-Test-p169253-uk33917

51 branches · 123 dependency updates · 5 security · 2 with artifact/lockfile problems

Title	Branch	Type	Change	Age	Notes
Update dependency @babel/core to v7.29.6 [SECURITY]	renovate/npm-babel-core-vulnerability	minor	7.19.1 → 7.29.6	106d	security
Update dependency browserslist to v4.28.7 [SECURITY]	renovate/npm-browserslist-vulnerability	minor	4.21.4 → 4.28.7	48d	security
Update dependency postcss to v8.5.29 [SECURITY]	renovate/npm-postcss-vulnerability	minor	8.4.16 → 8.5.29	45d	security
Update dependency webpack to v5.104.1 [SECURITY]	renovate/npm-webpack-vulnerability	minor	5.76.0 → 5.104.1	263d	security
Update dependency webpack-dev-server to v5 [SECURITY]	renovate/npm-webpack-dev-server-vulnerability	major	4.6.0 → 5.0.0	67d	security
Update dependency com.adobe.cq.core.wcm.components.core to v2.32.6	renovate/aem-core-components	minor	2.28.0 → 2.32.6	28d	
Update dependency com.adobe.aem-sdk-api to v2026.8.27830.20260820T160150Z-260700	renovate/aem-sdk-api	minor	2026.7.27293.20260724T150618Z-260600 → 2026.8.27830.20260820T160150Z-260700	12d	
Update dependency com.adobe.aem:aanalyzer-maven-plugin to v1.7.4	renovate/aemalyzer.version	minor	1.6.6 → 1.7.4	20d	
		minor		94d	

```
bisswang@bisswang-mb aem-cm-renovate % ./run-renovate-all.sh ../Ramon-Test-p169253-uk33917
>> repo: /Users/bisswang/git/aem-cloud/instances/renovate-test/Ramon-Test-p169253-uk33917
>> mode: DRY-RUN (no push)
>> [1/4] generating renovate/* branches...
>> [1/4] ensuring Gitea is up...
>> [2/4] mirroring Ramon-Test-p169253-uk33917 into Gitea...
remote: . Processing 1 references
remote: Processed 1 references in total
>> [3/5] running Renovate (creates branches; PRs land only in disposable Gitea)...
>> [4/5] fetching renovate/* branches into Ramon-Test-p169253-uk33917 (nothing pushed to real origin).
15 local renovate/* branches ready
>> [5/5] writing Markdown reports (PR body + release-notes/change history)...
wrote 15 report(s) + index.md
15 branches, 16 updates, 5 security
>> tearing down Gitea container (renovate-gitea)...
>> done.
>> reports: /Users/bisswang/git/aem-cloud/instances/renovate-test/aem-cm-renovate/renovate-
>> inspect branches: cd /Users/bisswang/git/aem-cloud/instances/renovate-test/Ramon-Test-p169253-uk3
>> delete local branches: ./cleanup-renovate-branches.sh /Users/bisswang/git/aem-cloud/instances/reno
>> [2/4] validating 15 branch(es) with 'mvn clean verify'...
>> (1/15) renovate/acorn-6.x ... PASS
>> (2/15) renovate/aemsync-4.x ... PASS
>> (3/15) renovate/autoprefixer-9.x ... PASS
>> (4/15) renovate/babel ... PASS
>> (5/15) renovate/com.adobe.cq.core.wcm.components.core ... PASS
```

Summary

- Keep dependencies current
 - automate dependency management
 - Validate + auto-merge where possible
- Combine updates with monitoring





adaptTo()

Appendix



- AEM Sites Optimizer
 - <https://experienceleague.adobe.com/en/docs/experience-manager-sites-optimizer/content/home>
- AEM MCP
 - <https://mcp.adobecloud.com/adobe/mcp/aem>
 - <https://experienceleague.adobe.com/en/docs/experience-manager-cloud-service/content/ai-in-aem/mcp-support/using-mcp-with-aem-as-a-cloud-service>