

TEAM SEVENFOLD

LEGACY PATCH INTELLIGENCE

# PatchPilot AI

레거시 패치 인텔리전스 — 업그레이드하지 못하는 시스템도, 그날에 대응한다

When a critical PHP CVE drops, PatchPilot tells you **which factory line is exposed** — and finds a **verified patch path for the EOL systems nobody can upgrade**.

## TARGET MARKET

US & EU industrial manufacturers  
running EOL PHP on OT lines

구형 PHP 7.4 HMI·MES 라인을 운영하는  
중견 제조사의 보안·설비팀 (Plant IT / OT  
Security)

## PROBLEM

"Just upgrade to 8.3" doesn't work on a  
production-line HMI. Teams can't prove  
exposure — or patch what vendors  
abandoned.

치명 RCE가 발표돼도 EOL 자산은 영향 판단도, 패  
치 경로도 없이 방치된다

## WHY NOW · PHP2SHELL

**CVSS 9.2** pre-auth RCE · every PHP since  
5.4

Found by AI in one week (Oct 21, 2026).  
Vulnerabilities arrive at AI speed —  
response must too.

AI가 발견하는 취약점의 시대 — 대응도 같은  
속도여야 한다

TRACK · Wildcard — AI Agent for Enterprise Security Operations

ANTHROPIC

서울특별시  
SEOUL METROPOLITAN GOVERNMENT

aihub  
SEOUL AI HUB



BASS  
VENTURES

AttentionX

Schmidt

springcamp

SV INVESTMENT

Goodwater

# What we built today

SBOM 업로드부터 EOL 백포트 계획·재현 증거까지 5단계 실제 동작 데모

PatchPilot AI — S3 Impact

S1 Import

S2 Intelligence

S3 Impact

S4 Workbench

S5 Report

Demo Mode · Synthetic Data

S3 · Impact — SBOM 매칭 · 자산별 위험

같은 CVE도 자산 상황(노출·중요도·EOU)에 따라 다르게 대응합니다. 점수는 데모용 정형 모델이며 CVSS가 아닙니다.

전체

Q. 자산 검색 (ID·이름)

6 / 6 자산

| ID     | 자산                                                                      | PHP    | 적용성      | 위험               | 상세 보기 |
|--------|-------------------------------------------------------------------------|--------|----------|------------------|-------|
| AS-001 | Supplier Portal (원격서 포털)<br>본사 DC · Docker (php8.3.35-apache)           | 8.3.35 | 강제 영향    | Risk 80 · HIGH   | 상세 보기 |
| AS-002 | MES Web Server (생산 실행)<br>1공장 · 온프레미스 VM (mod_php)                      | 8.2.34 | 강제 영향    | Risk 67 · MEDIUM | 상세 보기 |
| AS-003 | Quality Inspection HMI (품질검사) ★<br>2공장 검사라인 · 온프레미스 HMI 전용기 (구형 대체인 빌드) | 7.4.33 | 강제 영향    | Risk 78 · HIGH   | 상세 보기 |
| AS-004 | IoT Device Management (장치 관리)<br>본사 DC · Docker (php8.4.26-fpm)         | 8.4.26 | 강제 영향    | Risk 66 · MEDIUM | 상세 보기 |
| AS-005 | QA Report Server (테스트 리포트)<br>개발팀 · Docker (php8.3.36-fpm)              | 8.3.36 | 수정 버전 존재 | 점수 N/A           | 상세 보기 |
| AS-006 | PLC Firmware Controller (장치 제어)<br>2공장 라인 · 전용 펌웨어 (오프라인)               | PHP 없음 | 해당 없음    | 점수 N/A           | 상세 보기 |

잠재 영향 4 · 수정 버전 존재 1(AS-005) · 해당 없음 1(AS-006). 히어로 자산 AS-003은 EOL 백포트 경로로 분류됩니다.

AS-003 Legacy Workbench →

최근 활동

[04:41:02] 영향 분석 완료 — 4개 자산

[12:40:01] 리드 LEAD-01 → SOURCE\_REFERENCED

[12:39:00] Demo loaded · Synthetic enterprise data

## S3 · Impact — SBOM × CVE matching

6개 자산 자동 판정: 잠재 영향 4 · 수정 버전 1 · 미사용 1 + 자산별 위험 점수·근거 drawer

PatchPilot AI — S4 Workbench

S1 Import

S2 Intelligence

S3 Impact

S4 Workbench

S5 Report

Demo Mode · Synthetic Data

S4 · Legacy Backport Workbench — ★ 히어로

최신 버전 설치가 불가능한 설비에서 정확한 대안을 찾습니다. 선택 자산: AS-003

"The right patch is not always the newest version."

검증 전 백포 금지  
추진 후보(소스 백포트)는 출처만 확인됨(SOURCE\_REFERENCED) 상태입니다. 빌드·ABI 확장 모듈 회귀 검증과 OT 유지보수 장 승인 전까지 어떤 운영 환경에도 배포할 수 없습니다.

Legacy Environment

자산: Quality Inspection HMI (품질검사) ★ (AS-003)  
PHP: 7.4.33 EOL  
백포: 온프레미스 HMI 전용기 (구형 대체인 빌드)  
네트워크: SEGMENTED 분리 OT 구간  
제약: 구형 확장 모듈 · 구형 통제인 · 유지보수 장 제한  
PHP 7.4.33 품질검사 HMI 분리 OT 구간, 구형 확장 모듈 의존. 최신 PHP 즉시 교체 불가 — 데모 히어로.

현재 조치 상태  
채지 후보 식별  
백포트 후보는 "출처 확인(SOURCE\_REFERENCED)" 단계입니다. 빌드·ABI 회귀 검증 전까지 운영 적용 불가.

Patch Candidates (3)

1. 빌드 백포트  
7.4.33 → 미확정(빌드 확인 필요)  
빌드가 제공하는 패키지가 확인될 때만 후보로 승격된다.  
위험  
• 빌드 권고/패키지 근거가 아직 없음 — 임의 패키지 가장 금지  
검증 전제 (Prerequisites)  
• 빌드 보안 권고 확인  
• 패키지 서명/해시 검증  
UNVERIFIED

2. 소스 백포트 추천  
7.4.33 → 7.4.33+backport · commit 712a6019d1d — 소스 커밋 열기 — Official  
출처(커밋)는 확인됐지만 운영 검증 전까지 적용 불가 — SOURCE\_REFERENCED.  
위험  
• 새 펄퍼 zend\_mm\_safe\_error\_ex() 도입 — 구형 통제인 컴파일 검증 필요  
• 확장 모듈 ABI 재빌드 필요 (Zend 코어 변경 포함)  
• ext/session 변경 포함 — 세션 회귀 테스트 필요  
SOURCE\_REFERENCED  
검증 전제 (Prerequisites)

최근 활동

[12:41:00] AS-003 위험 78/HIGH

[12:40:01] 리드 LEAD-01 → SOURCE\_REFERENCED

[12:39:00] Demo loaded · Synthetic enterprise data

## S4 · Legacy Workbench — EOL 7.4 hero asset

소스 백포트 후보(php-src 커밋 근거) + 샌드박스 재현 EXPLOITED → BLOCKED 증거

S1 Import  
SBOM upload

→

S2 Verify  
OSINT ↔ official

→

S3 Impact  
per-asset risk

→

S4 Workbench  
backport plan

→

S5 Report  
exec summary

**WHERE CLAUDE WORKS** Every claim is grounded in official sources — php.net advisories, GHSA, php-src commits — separating **UNVERIFIED rumors** from **SOURCE\_REFERENCED facts**, then planning a verified source-backport for the EOL asset. 검증 상태가 UI 전체에 배지로 표시됩니다.

**Next 7 days:** multi-site SBOM ingest · vendor backport database · automated sandbox verification

ANTHROPIC

서울특별시  
SEOUL METROPOLITAN GOVERNMENT

aihub  
SEOUL AI HUB



BASS  
VENTURES

Attention

Schmidt

springcamp

SV INVESTMENT

Goodwater