PatchEMR

Automated Vulnerability &
Deployment Orchestrator for OpenEMR

CYSE 587

**Cyber Security
Systems Engineering**

George Mason University

Group 3

Shark Tank Seminar

April 2026

Chris Ghanma · Brandon Heiney · Megan Hoxha · Gabe Brinza · Bishesh Joshi · Sai Gudapati

01
THE PROBLEM

Hospitals & small clinics are afraid to patch their own software.

01 **Patch Paralysis**

Fear of downtime causes IT teams to delay upgrades for months which leaves known CVEs wide open in production.

02 **No Change Visibility**

Staff (especially in smaller clinics) have no way to compare security posture between OpenEMR versions before committing to an upgrade.

03 **HIPAA Exposure**

Running unpatched versions violates 45 CFR §164.308. Fines, legal liability, and loss of patient trust follow.

04 **Patient Risk**

EMR outages from ransomware have been directly linked to delayed care and increased patient mortality.

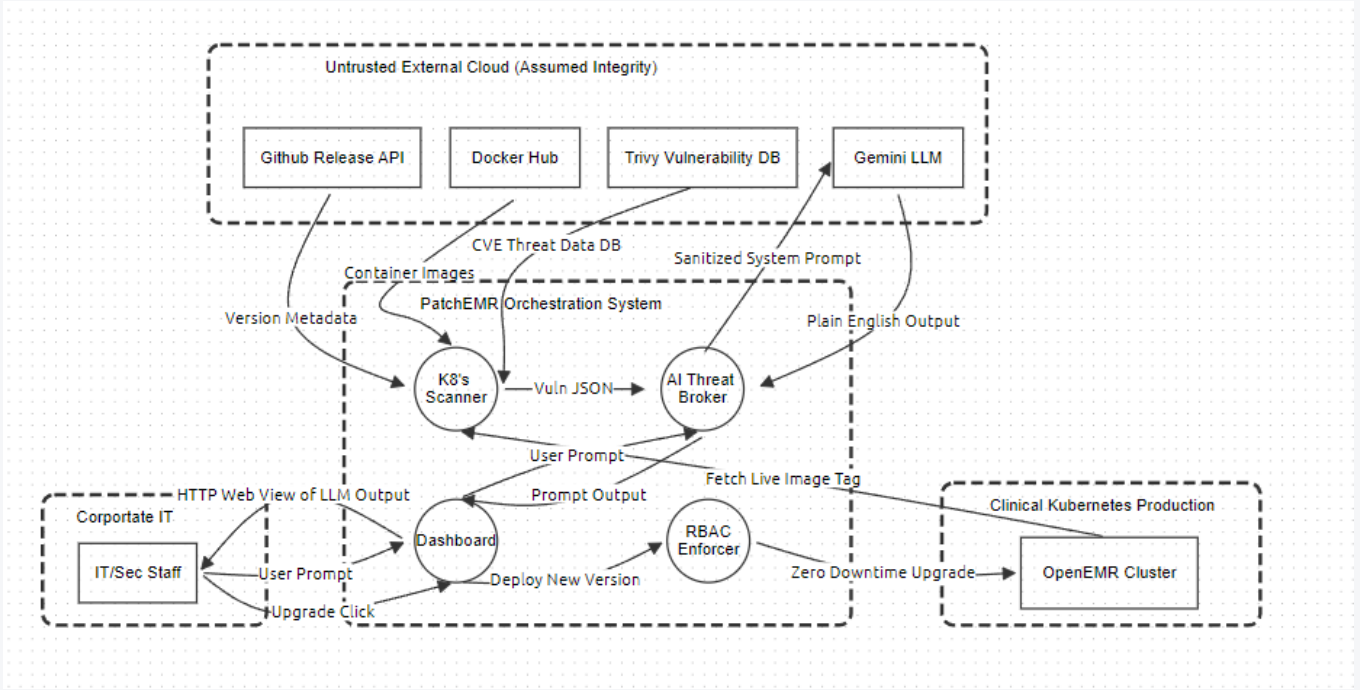
02
OUR SOLUTION

PatchEMR

An external deployment constraint system that validates every OpenEMR upgrade before it can reach the production cluster without touching a single line of its code.

Pre-Deployment Trivy Scan	Ephemeral Kubernetes pods scan both container images. No persistent scan infrastructure.
CVE Math Check	If Critical/High CVE count does not drop, deployment is blocked at the architecture level.
AI Threat Broker	Gemini LLM converts raw JSON CVE data into a plain-English GO/NO-GO executive summary.
RBAC Enforcer	Zero-downtime rolling Kubernetes update and upgrades if the authorization is given.

The Architecture



03

HOW IT WORKS

The Pipeline

1 Select Versions

IT/Clinician picks current production & proposed staging version from live environment & GitHub.

2 Trivy Scan

Ephemeral K8s pod pulls both images, outputs JSON of all Critical/High CVEs.

3 Math Check

Staging CVEs ≥ prod CVEs = deployment blocked. No exceptions and no overrides.

4 AI Summary

Gemini generates plain- English GO/NO-GO executive summary.

5 Authorize & Deploy

RBAC runs rolling K8s update. Zero downtime.

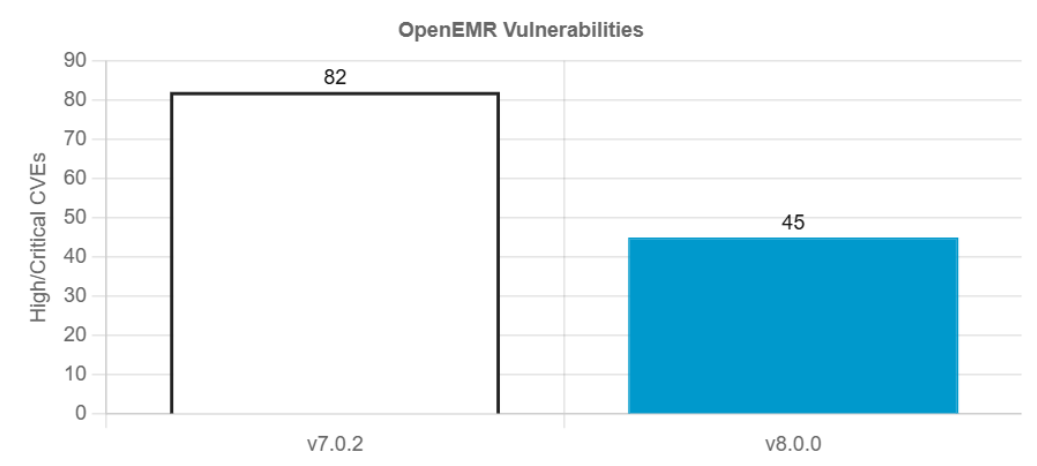
The AUTHORIZE button is hidden from the UI entirely when staging CVEs ≥ production CVEs and not just disabled, but also absent.

04

PROOF OF CONCEPT

It works.

Production v7.0.2 → Staging v8.0.0



82 Critical/High CVEs in production

45 After upgrade to v8.0.0

~45% Attack surface reduced

"This update dramatically reduces critical security risks from 82 to just 45, profoundly protecting patient data and minimizing disruptions to hospital operations." **- PatchEMR**

05

THREAT MODEL

STRIDE × Attack Tree

Threat Vector	Likelihood	Impact	CAPEC	Mitigation
Supply Chain Attack	Med-High	High	*CAPEC-184*	Math check is architectural and cannot be overridden even with compromised images.
Prompt Injection	Medium	High	*CAPEC-153*	RBAC ignores AI if math check fails. AI cannot deploy.
Insider Misuse	Low-Med	High	*CAPEC-560* *CAPEC-416*	Least-privilege dashboard with no raw kubectl for IT staff who do not need access.
Denial of Service	Medium	Low-Med	*CAPEC-469*	Pipeline DoS cannot take down the OpenEMR cluster, can only prevent upgrades because of a fully isolated boundary.

06
TRADE-OFFS

What we acknowledge.

RISK		CONTROL
Confidentiality	Gemini API receives CVE metadata with possible exposure if prompts aren't sanitized.	No PHI or internal network topology is transmitted due to lack of access to that information.
Integrity	Stale Trivy DB or compromised Docker Hub image could yield inaccurate scan results.	Math check is a hard architectural gate & AI alone cannot authorize a deployment.
Availability	Docker Hub outage stalls the pipeline when a critical patch is urgently needed.	Pipeline failure never takes down OpenEMR. Clusters are fully isolated from PatchEMR.
HIPAA §164.316	No log currently recorded for declined (NO-GO) upgrade decisions.	Fix: Implement audit log to record all NO-GO decisions with AI rationale attached.

07
STAKEHOLDERS

Who benefits.

01	**IT & Security Staff**	Replace guesswork with a clear GO/NO-GO verdict backed by scan data and an AI executive summary.
02	**Compliance Officers**	Every patch decision generates structured CVE evidence automatically which is audit-ready for HIPAA §164.308.
03	**Hospital Administrators**	Reduced regulatory exposure, zero unplanned downtime, and a repeatable process that doesn't need deep technical expertise.
04	**Clinicians & Patients**	OpenEMR stays online through every upgrade. Zero-downtime rolling Kubernetes updates mean no disruption to patient care workflows.

Demo!

Deploy the patch.

Not the risk.

PatchEMR converts patch paralysis into actionable assurance, giving every hospital, regardless of IT maturity, the confidence to keep OpenEMR secure and available.

Free & Open Source

No licensing cost

Non-Invasive

Never touches OpenEMR application

AI-Governed

Human + machine in the loop

github.com/OhDreadedDawn/PatchEMR

EXTRA SLIDES

ARCHITECTURE

Four trust boundaries. One enforcement point.

Untrusted External Cloud	GitHub Release API · Docker Hub · Trivy Vulnerability DB · Gemini LLM
PatchEMR Orchestration	Kubernetes Scanner · AI Threat Broker · Streamlit Dashboard · Math Enforcer
Corporate IT Zone	IT/Sec Staff · HTTP Web View · Upgrade Authorization Click
Clinical K8s Production	RBAC Enforcer → Zero-Downtime Rolling Update → OpenEMR Cluster

PatchEMR never touches OpenEMR source code, database schema, or clinical workflows. Integration is exclusively at the container orchestration layer via kubectl.