

# Healthcare Network Secures Its AngularJS Patient Portal with Seal Security

A regional healthcare network turned to Seal to secure the patient portal its patients use for appointments, lab results, care-team messages and billing, built on end-of-life AngularJS 1.8.3. With Claude Mythos surfacing open-source vulnerabilities at machine scale, no upstream fixes coming, and a rewrite in modern Angular estimated at close to three years, the network used Seal to remediate the AngularJS vulnerabilities in place.

## The Challenge

### ➤ End of support

AngularJS had reached end-of-life (EOL): Google no longer ships releases, and NVD notes the package will not receive fixes.

### ➤ Vulnerability risk

Claude Mythos now surfaces open-source vulnerabilities at machine scale. Known AngularJS CVEs, up to CVSS 7.5, let attackers phish patients inside the portal, track them, or freeze it.

### ➤ Compliance needs

HIPAA requires measures that reduce known risks to a reasonable level, and HHS has proposed hard patch deadlines. Open CVEs in a patient-facing portal would not meet that bar.

### ➤ Why the traditional fix is broken

The standard answer is to migrate to modern Angular. For a patient portal in daily use, that path is not viable:

- **Rewrite:** modern Angular is a different framework, so every screen of the portal has to be ported.
- **Time:** about 140 weeks for a 100,000-line app, with both frameworks in production meanwhile.
- **Cost:** about \$2.1M in engineering time, taken straight from the product roadmap.
- **Exposure:** every CVE stays open until the last AngularJS screen is gone.

# Seal's solution

Seal backported the fixes into the AngularJS release the portal already ran, with no rewrite.

## Angular rewrite vs Seal

### ✖ Rewrite path

angular 1.8.3 → open CVEs · up to CVSS 7.5 → rewrite in modern Angular

AngularJS is end-of-life upstream: no fixes for 1.x, so the only path is porting every screen to modern Angular, years of work.

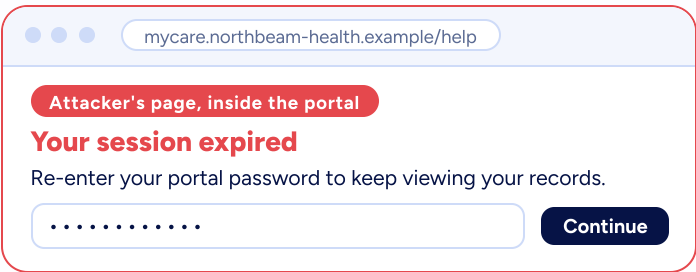
### ✔ Seal's approach

angular 1.8.3 → open CVEs · up to CVSS 7.5 → angular 1.8.3-sp1

Same release, same API, even on end-of-life AngularJS. 110 lines of AngularJS source changed, 0 lines of portal code, 7,700+ upstream tests passing.

**Delivered as a drop-in:** pulled from the Seal Artifact Server, validated against the portal's own regression suite, then published to the internal npm registry.

## The same phishing attack (CVE-2026-11998), two builds



✖ **Public 1.8.3:** the attacker gets Dana's password.



✔ **Seal 1.8.3-sp1:** link rejected. The attacker gets nothing.

## What 1.8.3-sp1 fixes, newest first

|                |                                                                       |            |       |
|----------------|-----------------------------------------------------------------------|------------|-------|
| CVE-2026-11998 | \$sce allowlist bypass: frames a fake sign-in page                    | GitHub 7.6 | Fixed |
| CVE-2025-0716  | Unsanitized SVG <image href>: loads attacker images                   | Snyk 6.3   | Fixed |
| CVE-2024-8372  | Image allowlist bypass in img[srcset]                                 | Snyk 6.3   | Fixed |
| CVE-2024-8373  | Unsanitized source[srcset]                                            | Snyk 6.3   | Fixed |
| CVE-2024-21490 | Freezes the page through ng-srcset                                    | CVSS 7.5   | Fixed |
| CVE-2023-26116 | Freezes angular.copy()                                                | CVSS 5.3   | Fixed |
| CVE-2023-26118 | Freezes <input type="url"> validation                                 | CVSS 5.3   | Fixed |
| CVE-2022-25844 | Freezes the currency filter. Open for 4.4 years with no upstream fix. | CVSS 5.3   | Fixed |

# The business impact with Seal

**110 lines**

of AngularJS source changed across all the fixes

**7,700+**

upstream AngularJS tests passing on the sealed build

**~140 weeks**

of rewrite avoided for a 100,000-line app (estimate)

**72 hrs**

Seal's SLA from disclosure to a sealed package

## Enhanced security

### Under 3 hours to a sealed build.

Known AngularJS CVEs up to CVSS 7.5 closed in place, including one open for 4.4 years.

## Compliance

**Evidence on day one.** Each fix is a reviewable patch with its own test, ready for the HIPAA risk file.

## Reduced operational disruption

**0 lines of portal code changed.** 140 weeks of rewrite replaced by one regression run.

## Cost savings

**About \$2.1M in rewrite cost avoided.** Engineering time kept for the product roadmap.

[LIVE DEMO · TRY IT YOURSELF](#)

## Attack the portal. Then switch on Seal.

Two copies of the same patient portal, one on public angular 1.8.3 and one on Seal's 1.8.3-sp1. Run the same attacks on both and see what the attacker gets.

1

### Steal a password

a fake sign-in page inside the portal

2

### Track who opens lab results

images loaded from the attacker

3

### Freeze the portal

one crafted value locks the page

Run it in your browser. [news.seal.security/angularjs-patient-portal](https://news.seal.security/angularjs-patient-portal)

[Open the demo](#)

Timeline from Seal's sealing run for angular 1.8.3-sp1. Rewrite estimate: lines of code divided by lines converted per week, times 1.4 (XLTS.dev), for 100,000 lines at 1,000 a week with four engineers at the US median developer wage of \$135,980 (BLS, May 2025) loaded to about \$194,000 a year (BLS ECEC, June 2026). Severity scores from NVD, GitHub and Snyk. HHS's patch deadlines are in the January 2025 proposed HIPAA Security Rule update and are not final.

[Book a demo](#) at [seal.security](https://seal.security)

