jscrambler

Security threats to healthcare apps

A data sheet by Jscrambler

Web healthcare platforms need in-depth security

Modern healthcare platforms leverage JavaScript code to provide the best possible user experience. However, **exposed JavaScript** helps attackers plan and automate attacks.

97%
Modern web apps Using JavaScript

100%
Fortune 500 Healthcare companies using JavaScript

87M
Patients in the US has their information breached in 2023

Attacks to healthcare platforms are growing

Because Protected Health Information (PHI) is valuable data, attackers go the extra mile to breach healthcare platforms. **Client-side security gaps provide an easy and silent way in.**

480
Data breaches in the US health care sector during the first three quarters of 2023

11M
The most significant breach recorded in 2023 was the HCA Healthcare breach. Affected 11 million individuals

$11M
Average cost of a health data breach

The threats to web healthcare platforms

Key business threats

Loss of customer data including protected health information (PHI) and user credentials.

Heavy HIPAA/ GDPR/CCPA fines following data breaches, which can amount to several hundred million dollars and lead to bankruptcy.

Lack of compliance with regulations and standards (HIPAA, NIST, ISO), namely in data protection and integrity policies.

Loss of customer trust, with clients terminating accounts following a data breach or fraudulent activity.

Client-side attacks in healthcare

Attacks to exposed JavaScript code

The JavaScript code that handles the logic of web healthcare platforms is exposed. Attackers can use this to easily understand how the application works and plan/automate data exfiltration or scraping attacks.

Magecart-like data breaches

It is very common for web platforms to rely on third-party code both during development and at runtime. Attackers can breach third-party code providers, injecting malicious code that will run on healthcare platforms, silently exfiltrating PHI.

Adware and malicious interface changes

By injecting malicious code into the client-side of web apps, attackers can display fake banners, leading end-users to malware, competitor websites, or fake mobile apps.

Intellectual property theft

Digital innovation is shaping the healthcare industry. Providers rely on JavaScript to develop high-performance web and mobile apps but, because client-side JavaScript is exposed, competitors can freely retrieve proprietary logic, putting competitive advantages at stake.

Most organizations have zero visibility and control of malicious app behavior

89%
Healthcare organizations experiencing data breaches.

79%
Healthcare organizations breached through third-party providers.

66%
Healthcare organizations saying cyberattacks have become more sophisticated

Healthcare meets client-side security

Key business threats

Minimize exposure to data breaches, by protecting JavaScript code and gaining real-time visibility of client-side attacks.

Increase compliance with regulations and standards such as HIPAA, GDPR, and NIST by preventing code tampering and stopping malicious app behavior.

Code Integrity protects the JavaScriptcode of your healthcare application

Enterprise-grade JavaScript protection
With Jscrambler's polymorphic JavaScript obfuscation, code locks, and self-defending capabilities, attackers won't be able to reverse-engineer, debug, or tamper with your code.

Robust countermeasures
Your application's code will detect debugging or tampering attempts and trigger countermeasures like breaking the application and notifying your security team in real-time.

Protect intellectual property and proprietary algorithms from the prying eyes of competitors or hackers.

Easily integrate with your SIEM to maximize your organization's ability to respond to threats in real-time.

Webpage Integrity secures your platform against malicious code

Full client-side visibility

Monitor the behavior of each of your website's scripts in real-time, see the full details of each detection and receive warnings for critical security threats.

Webpage threat mitigation

Mitigate client-side attacks to your website in real-time regardless of the attack vector and keep your users safe at all times. Prevent web supply chain attacks, data leakage, banking trojan webinjects, adware and customer hijacking.

References

L. Voss, “This year in JavaScript: 2018 in review and npm’s predictions for 2019”, December 6th, 2018, https://medium.com/npm-inc/this-year-in-javascript-2018-in-review-and-npms-predictions-for-2019-3a3d7e5298ef

npm Blog, “Managing JavaScript in the Enterprise”, February 21st, 2019, https://blog.npmjs.org/post/182958759735/managing-javascript-in-the-enterprise

Atlas VPN, Patient data breaches doubled, reaching 87M in 2023, October 18, 2023, https://atlasvpn.com/blog/patient-data-breaches-doubled-reaching-87m-in-2023

IBM Security, Cost of a Data Breach Report 2023, https://www.ibm.com/reports/data-breach

More than 88 million people have been affected by health data breaches this year, November 2, 2023, https://www.chiefhealthcareexecutive.com/view/more-than-88-million-people-have-been-affected-by-health-data-breaches-this-year

The HIPAA Journal, August 2023 Healthcare Data Breach Report, September 20, 2023, https://www.hipaajournal.com/august-2023-healthcare-data-breach-report/

If you want to know more about how Jscrambler can help you prevent client-side attacks, don’t hesitate to contact us.

hello@jscrambler.com | +1 650 999 0010