SEAL SECURITY

CASE STUDY:

Cybersecurity Asset Management Platform’s Journey to Becoming FedRAMP Compliant

The Backdrop

As a leading player in the cybersecurity asset management industry, this company offers platforms that empower IT and Security teams to understand and monitor the digital assets and infrastructure within an organization’s network. Their goal is to achieve and maintain FedRAMP compliance. Since the end of 2023, the company has faced significant challenges due to recurring vulnerabilities during their FedRAMP certification audit.

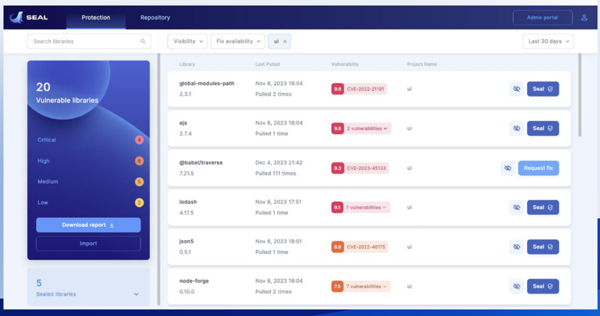
A Security Bottleneck

Achieving FedRAMP compliance is crucial for the company to service a vast market of government clients. The company utilizes two Linux distributions, Alpine Linux and Ubuntu, which are currently hindering their compliance due to security vulnerabilities. Particularly, critical and high-level vulnerabilities have been identified in Alpine Linux, related to third-party libraries. While their Software Composition Analysis (SCA) tool fails to detect all vulnerabilities, AWS does. The update process for these third-party fixes in Alpine Linux is slow, taking months to release updates.

Moreover, the company is challenged by using an outdated version of Ubuntu (Ubuntu 20), whereas the latest is Ubuntu 24. Upgrading poses risks of breaking existing functionalities, a common issue for many users stuck on older versions. This outdated version has vulnerabilities that are flagged during FedRAMP audits, pressuring the company to upgrade to the latest version and consider migrating from Alpine Linux to Ubuntu—a resource-intensive task requiring extensive time and resources.

Business Impact

Repeated failures in FedRAMP audits due to these vulnerabilities have resulted in lost business opportunities. The required upgrades and migration demand substantial time and resources from the development team, which could otherwise be directed towards innovation.



20 Vulnerable libraries

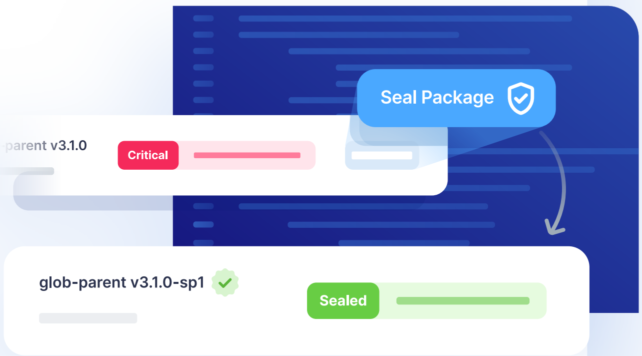
Critical	4
High	9
Medium	5
Low	2

5 Sealed libraries

Library	Last Pulled	Vulnerability	Project Name	
global-modules-path 2.3.1	Nov 8, 2023 18:04 Pulled 2 times	9.8 CVE-2022-21191	ui	Seal
ejs 2.7.4	Nov 8, 2023 18:04 Pulled 1 time	9.8 2 vulnerabilities	ui	Seal
@babel/traverse 7.21.5	Dec 4, 2023 21:42 Pulled 111 times	9.3 CVE-2023-45133	ui	Request fix
lodash 4.17.5	Nov 8, 2023 17:51 Pulled 1 time	9.1 7 vulnerabilities	ui	Seal
json5 0.5.1	Nov 8, 2023 18:01 Pulled 1 time	8.8 CVE-2022-46175	ui	Seal
node-forge 0.10.0	Nov 8, 2023 18:04 Pulled 2 times	7.5 7 vulnerabilities	ui	Seal

Turning Point with Seal Security

Thanks to the partnership with Seal Security, the cybersecurity company received patched versions for all vulnerabilities patches required by FedRamp within the first weeks of use and on a continuous basis. This swift response enabled them to pass the FedRAMP audit for their Linux distributions without the need for costly upgrades or migrations.



The Conclusion

With Seal Security's innovative solutions, the cybersecurity asset management company successfully overcame the challenges of FedRAMP compliance. The development team was able to concentrate on innovation and growth, while the security team confidently managed vulnerabilities. This success enabled the company to penetrate a new market, selling their services to government authorities, and ensuring a more secure future.

About Seal Security

Seal Security is the first AI solution for automated, scalable open source vulnerability remediation. This technology provides organizations with centralized control over the vulnerability patching process, eliminating the need for R&D team involvement. Offering standalone security patches in six programming languages, Seal Security ensures seamless and predictable remediation of vulnerabilities in direct and transitive dependencies, regardless of public maintainers' involvement. This enables security teams to respond immediately, reducing Mean Time to Repair (MTTR) from weeks to hours and significantly decreasing manual effort and technical debt.

AICPA Service Organization Control Reports AICPA SOC 2 Formerly SAS 70 Reports

INFORMATION SECURITY MANAGEMENT SYSTEM ISO 27001 CERTIFIED

For more information contact: info@sealsecurity.io