Verifying Product Security with Seamless Analysis of Product Binaries with Karamba's VCode

Case Study

Overview

Seagate Technology has been a global leader offering data storage and management solutions for over 40 years. Lyve™ Drive Mobile is yet another groundbreaking innovation from Seagate®: a high-capacity edge storage solution that enables businesses to aggregate, store, move and activate their data. Scalable, modular, and vendor agnostic, this integrated solution bundle eliminates network dependencies, so you can transfer mass data sets in a fast, secure and efficient manner. Pay only for the devices you need, when you need them.

Challenge

Ensure the security of Seagate shared storage software components, including third-party modules

Seagate Technology

Location

Seagate's new Lyve line of products tackles an important part of the storage market with no dedicated solutions. In order to shine in this area, the team wanted to have the best possible security posture for the solution. However, traditional IT software analysis tools can't analyze third party modules (provided as packaged binaries), which result in black boxes that could mask known vulnerabilities, embedded URLs, weak passwords and cybersecurity misconfigurations.

Having validation of strong security for the embedded controllers, including internally developed and third-party software modules, would allow Seagate's customers to safely share the device with stakeholders who should not access to the stored data.

Tel Aviv, Israel

Contact

seagate.com

Industry

Cyber Security

.

LYVE LABS™ ISRAEL

The Lyve Labs Israel team's mission is to connect external innovation in the Israeli ecosystem with Seagate's key challenges. When they learned of this security challenge, they set out to find IoT Security companies with mature solutions. That's how the connection was established with Karamba Security, who offers cutting-edge IoT Software Security solutions.

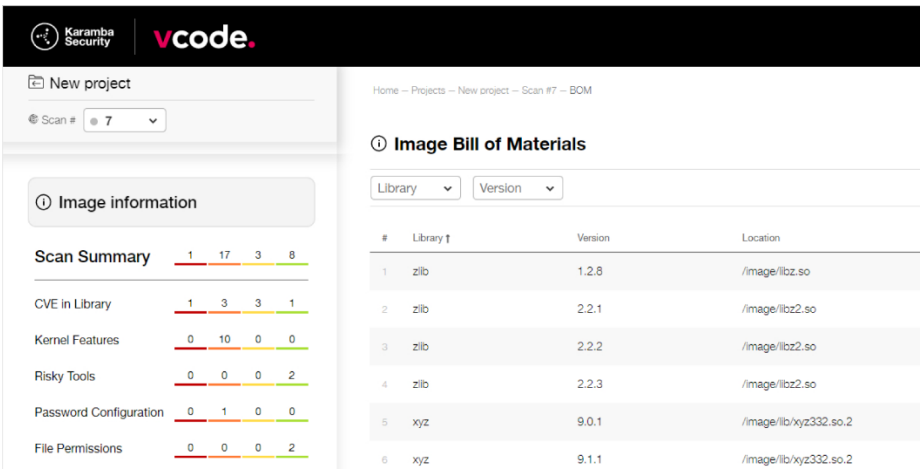
Karamba Security

Solution

Reveal software cyber risks, including 3rd party components, quickly and easily, by automatically unpacking and analyzing Seagate embedded software binaries, speeding up release cycles, and improving security posture and resiliency

Karamba Security's VCode automatically evaluates security vulnerability and security configuration issues with easy integration into the development CI/CD process. The issues are exposed for all software modules comprising the storage system, as all component libraries are detected and scanned automatically.

The deployment of VCode was seamless, as well as integrating it into existing security validation workflows across the software development process. Above all, the automation of the security validation that VCode enables made it instrumental in ensuring the entire Seagate image – consisting of internal and 3rd party components - has a consistently strong security posture.



Project in action:

Karamba Security's VCode solution integrated with Seagate's CI/CD process and allowed Product Security teams to quickly gain visibility into internally developed and 3rd party software components enable Seagate to improve the security posture of their solution. VCode saved significant time and money, and enabled Seagate to release more secure storage systems, that could meet its business goal of transporting customer data to the cloud.

Results

Provide actionable visibility into all software modules, including “black-box” 3rd party software, highlighting security issues that should be resolved prior to production release

Lyve Labs Israel, Seagate’s Innovation
Center was opened in February 2020 in Tel Aviv, Israel. Lyve Labs’ mission is to form partnerships with external innovation in the Israeli ecosystem in order to enable innovations by providing simple, secure, and efficient ways to work with exabytes of data. The initiative empowers the seamless movement of data, optimizing its business value both in flight and at rest.

When they found Karamba Security who offered a seamlessly integrated Software Security Assessment solution, they knew it could improve their developers’ experience as well as their ultimate release security posture.

"Karamba Security’s VCode enabled us to seamlessly analyze the cybersecurity posture of our software modules as well as third-party software modules. Thanks to VCode we know how to remediate the reported security issues before our storage systems go to production. Together with Karamba we have successfully implemented a Shift Left process, in which product security teams identify security issues, and direct our developers and third party, supply chain providers, to remediate them, before launching our storage products to the market.”

David Kaiser
Senior Director,
Product Security Office at
Seagate Technology