MINDING THE GAPS

The State of Vulnerabilities in Cloud Native Applications

The CNCF and Cloud Native Projects

The Cloud Native Computing Foundation is a sub-foundation of the Linux Foundation that supports and fosters the creation and adoption of cloud native technologies. Cloud native technologies help organizations grow and run solutions in cloud environments and on-premises architectures. They have certain characteristics, specifically, they are: scalable, dynamic, resilient, loosely coupled, manageable, observable, and automated. Some examples of cloud native applications are microservices, containers, and infrastructure as code. The group makes sure that these applications are well developed and robust enough to be used by many different organizations in production. It also identifies itself as a vendor-neutral home for many open-source projects. Currently, there are 16 graduated projects, 22 incubating projects, and a remaining 60 projects are at sandbox level. You can look at the complete CNCF landscape by checking https://l.cncf.io

The Security Audits

One particular working group inside the CNCF is the Security TAG team, or STAG. The STAG's objective is to facilitate collaboration for discovering and producing resources that enable secure access, policy control, and safety for operators, administrators, developers, and end-users across the cloud native ecosystem. One of the team's tasks is to request and coordinate independent security audits on cloud native projects. A list of the 2018-2020 security audits performed on these projects can be seen in Table 1.

Some of the security audit reports may be hard to find inside the repository of those projects. So, to make things easier, we've bundled them together into a unique location on this specific GitHub project with all the reports and assessments. We will try to keep this repository up to date as new security audits are released.

As seen in their list of security audits, the CNCF has been hiring independent security firms since 2018. Specifically, they have worked with Cure53, Trail of Bits, and AdaLogics. These groups analyze some of CNCFs projects, especially the more mature and widely adopted ones. The problem is that these are third-party consulting firms, and the final report usually comes in PDF files. These files are readable for human users; but they are hard to parse, and automating the results as issues on the project's issue tracker is also difficult. So, to analyze these results, we had to download all the files and parse through their results to collect the data in a standard format and store it in a single location for further analysis. After doing that, based on the data supplied and assembled from these security audit reports, we started doing some research and comparing the types and severity of vulnerabilities, among other things.

Project	Audit Date and Report	Announcement	Directed by	Audit Vendor
Kubernetes	08/06/2019	Announcement	CNCF (Security Audit WG)	Trail of Bits and Atredis Partners
Helm	11/04/2019	Announcement	CNCF (Security Audit WG)	Cure53 and Trail of Bits
gRPC	10/29/2019	Announcement	CNCF (Security Audit WG)	Cure53
etcd	08/05/2020	Announcement	CNCF (Security Audit WG)	Trail of Bits
rook	12/01/2019	Announcement	Project Maintainer	Trail of Bits
Fluentd	05/01/2019	Announcement	CNCF (Security Audit WG)	Cure53
Linkerd	06/01/2019	Announcement	CNCF (Security Audit WG)	Cure53

Project	Audit Date and Report	Announcement	Directed by	Audit Vendor
Harbor	10/01/2019	Announcement	CNCF (Security Audit WG)	Cure53
Falco	06/07/2019	Announcement	CNCF (Security Audit WG)	Cure53
TiKV	03/05/2020	Announcement	CNCF (Security Audit WG)	Cure53
NATS	02/06/2019	Announcement	CNCF (Security Audit WG)	Cure53
Prometheus	06/11/2018	Announcement	CNCF (Security Audit WG)	Cure53
CoreDNS	02/03/2018	Announcement	CNCF (Security Audit WG)	Cure53
Jaeger	05/04/2019	Announcement	CNCF (Security Audit WG)	Cure53
Vitess	02/01/2019	Announcement	CNCF (Security Audit WG)	Cure53
linkerd (rustls)	06/05/2020	Announcement	CNCF (Security Audit WG) + Buoyant	Cure53
OPA (gatekeeper)	03/10/2020	Announcement	CNCF (Security Audit WG)	Trail of Bits
Prometheus (node_exporter)	07/21/2020	Announcement	Project Maintainer	Cure53
FluentBit (fuzzing)	12/15/2020	Announcement	Project Maintainer	AdaLogics
Envoy	02/27/2018	Announcement	CNCF (Security Audit WG)	Cure53
TUF/Notary	08/07/2018	-	CNCF (Security Audit WG)	Cure53
OPA	08/30/2018	-	CNCF (Security Audit WG)	Cure53
Contour	12/01/2021	-	CNCF (Security Audit WG)	Cure53
linkerd (fuzzing)	05/07/2021	Announcement	CNCF	AdaLogics
Envoy (fuzzing)	05/14/2021	Announcement	CNCF	AdaLogics
Vitess (fuzzing)	05/19/2021	Announcement	CNCF	AdaLogics
SPIRE/SPIFFE	08/17/2021	Announcement	CNCF	Cure53

Table 1. CNCF Projects Security Audits List