Security Proposal to TSC

July 11, 2019

Agenda

- Security Tools
- Passing Criteria
- Plan

AKRAINO EDGE STACK

Security Tools

Test	Recommended tools	Notes
Source code static analysis	SonarQube	Open source. Community version free
Vulnerability analysis	Vuls	Open source, agent-less vulnerability scanner for Linux, FreeBSD
Full stack scan	Lynis	Open source security and auditing tool.

AKRAINO EDGE STACK

Passing Criteria

Severity	Definition	Pass Criteria		
		Incubation	Mature	Core
Critical	• Exploitation likely to result in root-level compromise; • Exploitation is usually straightforward		0	0
Important	• The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in a significant data loss or downtime.		<50%	<25%
Moderate	• Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.		<75%	<50%
Low	• Have *very little impact* on an organization's business. • Exploitation of such vulnerabilities usually requires local or physical system access.			

AKRAINO EDGE STACK

https://www.atlassian.com/trust/security/security-severity-levels

%: not-fixed/found

Plan

- When to start?
  - Now
- Tracking and enforcement
  - Security check logs are pushed to a persistent storage
  - Key metrics will be captured and shown in portal for each project
  - PTLs are invited to security sub-committee meeting for status check periodically
  - Security sub-committee reports to TSC about security status periodically

AKRAINO EDGE STACK

For More Information, Please
Visit www.akraino.org