

Akraino Release SDL Requirements Matrix

Release Tags:

- tc:approved-release
- stable:follows-policy
- assert:supports-upgrade
- assert:supports-accessible-upgrade
- assert:supports-rolling-upgrade
- assert:follows-standard-deprecation

There are 3 fields in a numbered release tag: 0.1.1, where first follows even numbers for stable release, odd numbers for development release for big changes; second follows even numbers for stable release, odd numbers for development release for small updates; third field follows by non-negative numbers for each patch version.

Phases	Requirements	Release 1 Feature Project	Release 1 Integration Project
Requirements	Determine if the project is subject to SDL policy	X	X
	Identify security advisor and security champion	X	
	Define security bug bar	X	X
	Bug tracking tool must have Security Bug Effect field and Security Bug Cause field	X	
	Security and privacy risk assessment	X	
	Write Security plan document		
Design	Security design review	X	
	Threat modeling	X	X
	Follow cryptograph requirements	X	X
	Write security architecture document		
	Minimize default attack surface		
	Enable least privilege	X	X
	Default secure	X	X
	Consider a defense-in-depth approach		
	Examine past vulnerabilities in previous version of the project		
	Deprecate outdated functionality		
	Conduct a security review of source code		
	Ensure appropriate logging	X	X
	Hardware security design review		
	Enforce strong log-out and session management		
	Follow NEAT security user experience guidance		
	Improve security-related prompts		
Implementation	Establish and follow best practices	X	X
	Run static analysis tool	X	X
Validation	Dynamic analysis	X	
	Fuzz testing (File parsing, RPC, network)	X	X
	Kernel-model driver test	X	X
	Risk and attack surface review		
	Cross-site scripting testing	X	X
	Penetration test		
	Binary analysis		

	Vulnerability regression test		
	Data flow test		
	Reply test		
	Input validation test (Symbolic Execution)		
	Privacy Model Checking (Information Flow Self-Composite Verification)		
	Secure code review		
	Security push		
Release	Incident and response plan	X	X
	Review and update the privacy companion form	X	X
	Complete the privacy disclosure	X	X
	Final security and privacy review	X	
	Patch deployment tools	X	X
	Release note with security disclosure	X	X