Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi

Received Date : 12/17/2023 10:26 AM

Comments Received :

Section III, clause 4

We suggest to extend clause 4 b), as following (suggested changes marked in ***):

b) The software producer has a policy or process to address discovered *** and relevant *** security vulnerabilities *** based on the software producer risk assessment and policies *** prior to product release;

Rationale:
Not all discovered security vulnerabilities are actually a risk to the produced software (eg non reachable dependencies, non deployed software, non valid secrest). It IS crucial to assure that the relevant vulnerabilities are fixed before going to production. Relevant vulnerabilities are the ones that pass the risk bar of the software producer after performing risk calculations for each vulnerability based on estimating the likelihood of its exploitability, the potential impact if exploited, and any other relevant characteristics.
This approach is directly aligned with RV.2 in SSDF Practices and Tasks and especially with:
-- RV.2.1: Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response.
-- RV.2.2: Plan and implement risk responses for vulnerabilities.