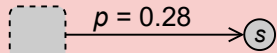
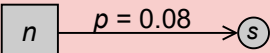


# Proposed risk rules

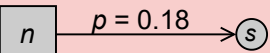
**Risk rule CVE-2021-40830:** IF software component  $s$  was compiled with SDK which contains vulnerability **THEN** create a risk edge from an *entryvertex* to  $s$  with the exploitation probability  $p = 0.28$ .



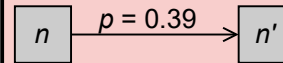
**Risk rule CVE-2022-25666:** IF software component  $s$  is deployed on node  $n$  **AND**  $n$  contains firmware with vulnerability **THEN** create a risk edge from  $n$  to  $s$  with the exploitation probability  $p = 0.08$ .



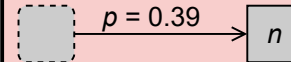
**Risk rule CVE-2021-22547:** IF software component  $s$  is deployed on node  $n$  **AND**  $s$  was compiled with SDK which contains vulnerability **THEN** create a risk edge from  $n$  to  $s$  with the exploitation probability  $p = 0.18$ .



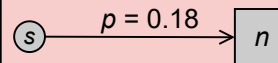
**Risk rule CVE-2022-35927:** IF two nodes  $n, n'$  are connected via a link **AND**  $n'$  contains an outdated version of Contiki-NG OS **THEN** create a risk edge from  $n$  to  $n'$  with the exploitation probability  $p = 0.39$ .



**Risk rule CVE-2022-35927:** IF node  $n$  contains version of Contiki-NG OS with vulnerability **THEN** create a risk edge from an *entryvertex* to  $n$  with the exploitation probability  $p = 0.39$ .




**Risk rule CVE-2020-3676:** IF software component  $s$  is deployed on node  $n$  **AND**  $n$  contains firmware with vulnerability **THEN** create a risk edge from  $s$  to  $n$  with the exploitation probability  $p = 0.18$ .



## Legend

 = Node in attack graph    = Entry vertex    = Software component in attack graph

 = Risk edge with an exploitation probability  $p$