Release 5 Blueprint Scanning Status

Approved Blueprints

	Project Name	**Vuls Scan** • Pass/Fail • Exceptions	**Lynis Scan** • Pass/Fail • Exceptions	**Kube-Hunter Scan** • Pass/Fail • Exceptions
1	ELIOT SD-WAN /WAN Edge/uCPE Blueprint			The following exceptions must be fixed prior to maturity review: 1. CAP_NET_RAW Enabled - CAP_NET_RAW is enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node.
2	Enterprise Applications on Lightweight 5G Telco Edge			The following exceptions must be fixed prior to maturity review: 1. CAP_NET_RAW Enabled - CAP_NET_RAW is enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node.
3	Public Cloud Edge Interface (PCEI) Blueprint		The following exceptions must be fixed prior to maturity review: 1. test ID AUTH-9328 (Default umask values) Reason: <Oleg Berzin> Cannot fix AUTH-9328 because changing unmask value to 027 caused lynis test suite to fail (does not run)	The following exceptions must be fixed prior to maturity review: 1. CAP_NET_RAW Enabled - CAP_NET_RAW is enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node.
4	The AI Edge: Federated ML application at edge	Release 5: Akraino CVE Vulnerability Exception Request		
5	KNI Provider Access Edge			The following exceptions must be fixed prior to maturity review: 1. CAP_NET_RAW Enabled - CAP_NET_RAW is enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node.
6	KNI Industrial Edge			The following exceptions must be fixed prior to maturity review: 1. CAP_NET_RAW Enabled - CAP_NET_RAW is enabled by default for pods. If an attacker manages to compromise a pod, they could potentially take advantage of this capability to perform network attacks on other pods running on the same node.
7	IEC Type 2 for Integrated Edge Cloud (IEC) Blueprint Family			the security issues observed seem to be specific to microk8s cluster. We ran the sonobuoy tests & kube-hunter against k3s and there are no issues in the master setup. We are working with Canonical to review our configuration. The following exceptions must be fixed prior to maturity review: 1. Information Disclosure: Exposed pods. An attacker could view sensitive information about pods that are bound to a Node using the /pods endpoint. 2. KHV043 (Information Disclosure): Cluster Health Disclosure. By accessing the open /healthz handler, an attacker could get the cluster health state without authenticating. 3. KHV044 (Access Risk): Pivileged Container. A privileged container exists on a node, could expose the node /cluster to unwanted root operations.
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				

23				
24				
25				
26				
27				
28				
29				
30				
31				
32				