Release 4 Blueprint Scanning Status

Approved Blueprints

	Project Name	Vuls Scan • Pass/Fail • Exceptions	Lynis Scan • Pass/Fail • Exceptions	Kube-Hunter Scan • Pass/Fail • Exceptions
1	5G MEC/Slice System to Support Cloud Gaming, HD Video and Live Broadcasting Blueprint	Release 4 Vuls Exception Request	The following exceptions must be fixed prior to maturity review: 1. Performing test ID USB-2000 (Check USB authorizations) 2. Performing test ID PKGS-7370 (Checking for debsums utility) 3. sysctl key net.ipv4.conf.all.rp_filter contains equal expected and current value (1)	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	AI/ML and AR/VR applications at Edge	Release 4 Vuls Exception Request		
3	Connected Vehicle Blueprint	Release 4 Vuls Exception Request	1. Consider hardening SSH configuration [test:SSH-7408] [details: Port (set 22 to) Exception is granted for using port 22 for testing/BlueVal. However, since this BP is requesting a maturity review the port must be changed to a high port after testing for production use. 2. Consider hardening SSH configuration [test:SSH-7408] [details:MaxSessions (set 4 to 2) Exception is granted for testing /BlueVal. Since this BP is requesting a maturity review the MaxSessions must be changed to 2 after testing for production use.	
4	Edge Video Processing	Release 4 Vuls Exception Request		
5	ELIOT: Edge Lightweight and IoT Blueprint Family	Release 4 Vuls Exception Request		
6	• ELIOT AIoT in Smart Office Blueprint	Release 4 Vuls Exception Request		

| 7 | • ELIOT IoT Gateway Blueprint | Release 4 Vuls Exception Request | 1. Performing test ID BOOT-5122 (Check for GRUB boot password) ## After setting up grub boot password --> Cloud Vms won't boot properly. Lead to unstable VMs
2. Performing test ID AUTH-9229 (Check password hashing methods) ## Not possible, will impact SHA_MIN_CRYPT_ROUNDS test. Currently using maximum security hashing method SHA512
3. Performing test ID USB-2000 (Check USB authorizations) ## N/A: Using cloud VMs, no baremetal involved.
4. Performing test ID USB-3000 (Check for presence of USBGuard) ## N/A: Using cloud VMs, no baremetal involved.
5. Test: Checking MaxSessions ## Max session set to 4, this is the bare minimum level that can be used.
6. Test: Checking Port ## Can't change during testing, BluVal requires SSH to be tcp/22. This port should be changed after testing, but prior to production.
7. KRNL-6000: sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 ## IP Forwarding is required for K8s.

The following exceptions must be fixed prior to maturity review:

1. sysctl key kernel.core_uses_pid contains equal expected and current value (1)
2. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0
3. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16
4. sysctl key net.ipv4.conf.all.log_martians contains equal expected and current value (1)
5. sysctl key net.ipv4.conf.all.send_redirects contains equal expected and current value (0)
6. sysctl key net.ipv4.conf.default.accept_redirects contains equal expected and current value (0)
7. sysctl key net.ipv4.conf.default.log_martians contains equal expected and current value (1)
8. sysctl key net.ipv6.conf.all.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1
9. sysctl key net.ipv6.conf.default.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 | 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. |

| 8 | • ELIOT SD-WAN /WAN Edge/uCPE Blueprint | Release 4 Vuls Exception Request | The failed test below in Lynis is granted an exception because ip forwarding is required in deployments using Kubernetes:

1. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1

The following additional exceptions are granted for this blueprint:

1. Performing test ID AUTH-9229 (Check password hashing methods) ## Not possible, will impact SHA_MIN_CRYPT_ROUNDS test. Currently using maximum security hashing method SHA512
2. Performing test ID USB-2000 (Check USB authorizations) ## N/A: Using cloud VMs, no baremetal involved.
3. Performing test ID USB-3000 (Check for presence of USBGuard) ## N/A: Using cloud VMs, no baremetal involved.
4. Test: Checking MaxSessions ## Max session set to 4, this is the bare minimum level that can be used.
5. Test: Checking Port ## Can't change during testing, BluVal requires SSH to be tcp/22. This port should be changed after testing, but prior to production.
6. KRNL-6000: sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 ## IP Forwarding is required for K8s.

The following exceptions must be fixed prior to maturity review:

1. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0
2. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16
3. sysctl key kernel.yama.ptrace_scope has a different value than expected in scan profile. Expected=1 2 3, Real=0
4. sysctl key net.ipv4.conf.all.log_martians contains equal expected and current value (1)
5. sysctl key net.ipv4.conf.all.send_redirects contains equal expected and current value (0)
6. sysctl key net.ipv4.conf.default.accept_redirects contains equal expected and current value (0)
7. sysctl key net.ipv4.conf.default.log_martians contains equal expected and current value (1)
8. sysctl key net.ipv6.conf.all.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1
9. sysctl key net.ipv6.conf.default.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 | 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. |

9	Network Cloud and TF Integration Project	Release 4 Vuls Exception Request	The failed test below in Lynis is granted an exception because ip forwarding is required in deployments using Kubernetes: 1. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 Below are items found in lynis that are granted an exception due to Release 3 considerations, however, these must be fixed prior to incubation (or maturity) in next Release. 1. Test ID BOOT-5122 (Check for GRUB boot password) 2. PASS_MAX_DAYS option in /etc/login.defs 3. Test ID AUTH-9328 (Default umask values) 4. Test ID SSH-7440 (Check OpenSSH option: AllowUsers and AllowGroups) 5. sysctl key fs.suid_dumpable contains equal expected and current value (0) 6. sysctl key kernel.dmesg_restrict contains equal expected and current value (1) Below are items found in lynis that can be granted an exception, but must be fixed prior to maturity: 1. Performing test ID USB-3000 (Check for presence of USBGuard) 2. Test: Checking MaxSessions in /tmp/lynis.ZotHQ7RQAj 3. Test: Checking Port in /tmp/lynis.ZotHQ7RQAj 4. sysctl key kernel.core_uses_pid contains equal expected and current value (1)	Approved with exceptions, since prior to maturity. Upgrading K8s components causes the Airship deployment to fail and the regional controller becomes incompatible. The development team was told to use a specific version of the regional controller and airship (as the older versions are stable and newer are in flux and fragile). When the team upgraded to the new version as per the security team's suggestion, everything else fell apart. Making this change will require several months of work as the development team has to upgrade a component at a time to bring everything to the latest version of code.
10	Integrated Cloud Native NFV/App stack family (Short term: ICN)	Release 4 Vuls Exception Request	The failed test below in Lynis is granted an exception because ip forwarding is required in deployments using Kubernetes: 1. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 Below are items found in lynis that can be granted an exception, but must be fixed prior to maturity: 1. Performing test ID USB-3000 (Check for presence of USBGuard) 2. Test: Checking MaxSessions in /tmp/lynis.ZotHQ7RQAj 3. Test: Checking Port in /tmp/lynis.ZotHQ7RQAj	
11	Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request		
12	• IEC Type 1 for Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request		
13	• IEC Type 2 for Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request		

14	• IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request	The following exceptions must be fixed prior to maturity review: 1. Performing test ID AUTH-9229 (Check password hashing methods) 2. Test: Checking SHA_CRYPT_MIN_ROUNDS option in /etc/login.defs 3. Performing test ID USB-2000 (Check USB authorizations) 4. Performing test ID USB-3000 (Check for presence of USBGuard) 5. Performing test ID PKGS-7370 (Checking for debsums utility) 6. Test: Checking AllowTcpForwarding in /tmp/lynis.ZotHQ7RQAj 7. Test: Checking ClientAliveCountMax in /tmp/lynis.ZotHQ7RQAj 8. Test: Checking MaxAuthTries in /tmp/lynis.ZotHQ7RQAj 9. Test: Checking MaxSessions in /tmp/lynis.ZotHQ7RQAj 10. Test: Checking Port in /tmp/lynis.ZotHQ7RQAj 11. Test: Checking TCPKeepAlive in /tmp/lynis.ZotHQ7RQAj 12. sysctl key kernel.core_uses_pid test must pass 13. sysctl key kernel.kptr_restrict test must pass 14. sysctl key kernel.sysrq test must pass 15. sysctl key net.ipv4.conf.all.forwarding test must pass 16. sysctl key net.ipv4.conf.all.log_martians test must pass 17. sysctl key net.ipv4.conf.all.send_redirects test must pass 18. sysctl key net.ipv4.conf.default.accept_redirects test must pass 19. sysctl key net.ipv4.conf.default.log_martians test must pass 20. sysctl key net.ipv6.conf.all.accept_redirects test must pass 21. sysctl key net.ipv6.conf.default.accept_redirects test must pass	Kubernetes not used.
15	• IEC Type 4: AR/VR oriented Edge Stack for Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request	The following exceptions must be fixed prior to maturity review: 1. Test ID AUTH-9229 (Check password hashing methods)	Kubernetes not used.
16	• IEC Type 5: SmartNIC for Integrated Edge Cloud (IEC) Blueprint Family	Release 4 Vuls Exception Request	The following exceptions must be fixed prior to maturity review: 1. Test ID AUTH-9229 (Check password hashing methods) 2. Test: Checking SHA_CRYPT_MIN_ROUNDS option in /etc/login.defs 3. Test ID USB-2000 (Check USB authorizations) 4. Test ID USB-3000 (Check for presence of USBGuard) 5. Test: Checking AllowTcpForwarding in /tmp/lynis.ZotHQ7RQAj 6. Test: Checking ClientAliveCountMax in /tmp/lynis.ZotHQ7RQAj 7. Test: Checking MaxAuthTries in /tmp/lynis.ZotHQ7RQAj 8. Test: Checking MaxSessions in /tmp/lynis.ZotHQ7RQAj 9. Test: Checking Port in /tmp/lynis.ZotHQ7RQAj 10. Test: Checking TCPKeepAlive in /tmp/lynis.ZotHQ7RQAj 11. sysctl key kernel.kptr_restrict test must pass 12. sysctl key kernel.sysrq test must pass 13. sysctl key kernel.yama.ptrace_scope test must pass 14. sysctl key net.ipv4.conf.all.forwarding test must pass 15. sysctl key net.ipv4.conf.all.log_martians test must pass 16. sysctl key net.ipv4.conf.default.log_martians test must pass	Kubernetes not used.
17	Kubernetes-Native Infrastructure (KNI) Blueprint Family	Release 4 Vuls Exception Request		

| 18 | • KNI Provider access edge | | The following exceptions must be fixed prior to maturity review:

1. Test: Checking presence /var/run /reboot-required.pkgs
2. Performing test ID AUTH-9228 (Check password file consistency with pwck)
3. Test: Checking SHA_CRYPT_MIN_ROUNDS option in /etc/login.defs
4. Performing test ID USB-2000 (Check USB authorizations)
5. Performing test ID USB-3000 (Check for presence of USBGuard)
6. Test: Checking AllowTcpForwarding in /tmp/lynis.ZotHQ7RQAj
7. Test: Checking ClientAliveCountMax in /tmp/lynis.ZotHQ7RQAj
8. Test: Checking MaxAuthTries in /tmp /lynis.ZotHQ7RQAj
9. Test: Checking MaxSessions in /tmp /lynis.ZotHQ7RQAj
10. Test: Checking Port in /tmp/lynis. ZotHQ7RQAj
11. Test: Checking TCPKeepAlive in /tmp /lynis.ZotHQ7RQAj
12. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0
13. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16
14. sysctl key kernel.yama.ptrace_scope has a different value than expected in scan profile. Expected=1 2 3, Real=0
15. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1
16. sysctl key net.ipv4.conf.all. log_martians contains equal expected and current value (1)
17. sysctl key net.ipv4.conf.all. send_redirects contains equal expected and current value (0)
18. sysctl key net.ipv4.conf.default. accept_redirects contains equal expected and current value (0)
19. sysctl key net.ipv4.conf.default. log_martians contains equal expected and current value (1)
20. sysctl key net.ipv6.conf.all. accept_redirects has a different value than expected in scan profile. Expected=0, Real=1
21. sysctl key net.ipv6.conf.default. accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 | 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. |

19	• KNI Industrial Edge		The following exceptions must be fixed prior to maturity review: 1. Test: Checking presence /var/run /reboot-required.pkgs 2. Performing test ID AUTH-9228 (Check password file consistency with pwck) 3. Test: Checking SHA_CRYPT_MIN_ROUNDS option in /etc/login.defs 4. Performing test ID USB-2000 (Check USB authorizations) 5. Performing test ID USB-3000 (Check for presence of USBGuard) 6. Test: Checking AllowTcpForwarding in /tmp/lynis.ZotHQ7RQAj 7. Test: Checking ClientAliveCountMax in /tmp/lynis.ZotHQ7RQAj 8. Test: Checking MaxAuthTries in /tmp /lynis.ZotHQ7RQAj 9. Test: Checking MaxSessions in /tmp /lynis.ZotHQ7RQAj 10. Test: Checking Port in /tmp/lynis. ZotHQ7RQAj 11. Test: Checking TCPKeepAlive in /tmp /lynis.ZotHQ7RQAj 12. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0 13. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16 14. sysctl key kernel.yama.ptrace_scope has a different value than expected in scan profile. Expected=1 2 3, Real=0 15. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 16. sysctl key net.ipv4.conf.all. log_martians contains equal expected and current value (1) 17. sysctl key net.ipv4.conf.all. send_redirects contains equal expected and current value (0) 18. sysctl key net.ipv4.conf.default. accept_redirects contains equal expected and current value (0) 19. sysctl key net.ipv4.conf.default. log_martians contains equal expected and current value (1) 20. sysctl key net.ipv6.conf.all. accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 21. sysctl key net.ipv6.conf.default. accept_redirects has a different value than expected in scan profile. Expected=0, Real=1	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.
20	Micro-MEC	Release 4 Vuls Exception Request		
21	The AI Edge: School /Education Video Security Monitoring	Release 4 Vuls Exception Request	The following items must be fixed for incubation or maturity in the next release: 1. Test ID HRDN-7220 (Check if one or more compilers are installed) ; /usr /bin/as compiler was found and must be removed 2. Test ID AUTH-9328 (Default umask values) The following items must be fixed for maturity approval, these tests and results can be found in the lynis.log file: 1. Test ID BOOT-5184 2. Test: Checking presence /var/run /reboot-required.pkgs 3. Test ID AUTH-9229 (Check password hashing methods) 4. Test: Checking Port in /tmp/lynis. ZotHQ7RQAj; ssh port can not be set to tcp/22. 5. sysctl key kernel.sysrq ; Must be expected value 6. sysctl key net.ipv4.conf.all.forwarding ; Must be expected value	Following exception granted (this issue is being investigated as possibly fixed in next version of kube-hunter): 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. The following items must be fixed prior to the next release, these tests and results can be found in the cluster.log file: 1. KHV005 - Unauthenticated access to API 2. KHV002 - K8s Version Disclosure The following items must be fixed prior to the next release, these tests and results can be found in the pod.log file: 1. Access to pod's secrets. Accessing the pod's secrets within a compromised pod might disclose valuable data to a potential attacker. 2. KHV050 - Read access to pod's service account token. Accessing the pod service account token gives an attacker the option to use the server API.
22	Network Cloud Blueprint Family	Release 4 Vuls Exception Request		
23	StarlingX Far Edge Distributed Cloud	Release 4 Vuls Exception Request		
24	Telco Appliance Blueprint Family	Release 4 Vuls Exception Request		

25	• Radio Edge Cloud (REC)	Release 4 Vuls Exception Request	1. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile - Required by kubernetes 2. Test ID USB-2000 (Check USB authorizations - USB required for installation occurs via virtual devices presented as USB; virtual console requires USB; USB is also used for emergency on-site access. 3. Test: Checking Port tcp/22 - Ansible driven installs use tcp/22; current operations support model uses ssh on tcp/22. 4. HRDN-7220 AS compiler exists, however, in HRDN-7222 symlink to AS compiler has been removed.	Following exception granted (this issue is being investigated as possibly fixed in next version of kube-hunter): 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.
26	• SDN Enabled Broadband Access (SEBA) for Telco Appliance Blueprint Family	Release 4 Vuls Exception Request		
27	The AI Edge Blueprint Family	Release 4 Vuls Exception Request		
28	Time-Critical Edge Compute	Release 4 Vuls Exception Request		
29	Public Cloud Edge Interface (PCEI)	Release 4 Vuls Exception Request	the following exception was granted based on the input provided by Blueprint owner: 1. Performing test ID AUTH-9328 (Default umask values) When I try to change the UNMASK value from 022 to recommended 027 on the SUT – the Lynis tests stop working, with an error the files in /var/log/ do not exist. So I could not address this issue - Oleg Berzin The following exceptions must be fixed prior to maturity review: 1. Test: Checking presence /var/run/reboot-required.pkgs 2. Test: Checking SHA_CRYPT_MIN_ROUNDS option in /etc/login.defs 3. Performing test ID USB-2000 (Check USB authorizations) 4. Performing test ID USB-3000 (Check for presence of USBGuard) 5. Performing test ID PKGS-7370 (Checking for debsums utility) 6. Test: Checking AllowTcpForwarding in /tmp/lynis.ZotHQ7RQAj 7. Test: Checking ClientAliveCountMax in /tmp/lynis.ZotHQ7RQAj 8. Test: Checking MaxAuthTries in /tmp/lynis.ZotHQ7RQAj 9. Test: Checking MaxSessions in /tmp/lynis.ZotHQ7RQAj 10. Test: Checking Port in /tmp/lynis.ZotHQ7RQAj 11. Test: Checking TCPKeepAlive in /tmp/lynis.ZotHQ7RQAj 12. sysctl key kernel.core_uses_pid contains equal expected and current value (1) 13. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0 14. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16 15. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 16. sysctl key net.ipv4.conf.all.log_martians contains equal expected and current value (1) 17. sysctl key net.ipv4.conf.all.send_redirects contains equal expected and current value (0) 18. sysctl key net.ipv4.conf.default.accept_redirects contains equal expected and current value (0) 19. sysctl key net.ipv4.conf.default.log_martians contains equal expected and current value (1) 20. sysctl key net.ipv6.conf.all.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 21. sysctl key net.ipv6.conf.default.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1	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.

30	Enterprise Applications on Lightweight 5G Telco Edge	Release 4 Vuls Exception Request	1. Performing test ID BOOT-5122 (Check for GRUB boot password) - Granted an exception because Blueprint is using a public cloud VM and GRUB password cannot be changed. 2. Performing test ID AUTH-9229 (Check password hashing methods) - Exception granted: output provided showing both root and non-root hashing set to SHA512 and 800,000 rounds. 3. Performing test ID USB-2000 (Check USB authorizations) - Exception granted because not possible since using cloud VM 4. Test: Checking MaxSessions - Exception granted reduced from MaxSessions --> 6 to 4. Minimum 4 sessions are needed for BluVal to run 5. Test: Checking Port - Exception granted; Validation framework is failing if ssh changed from Port 22 --> {}. Needed for BlueVal to run. The following exceptions must be fixed prior to maturity review: 1. sysctl key kernel.core_uses_pid contains equal expected and current value (1) 2. sysctl key kernel.kptr_restrict has a different value than expected in scan profile. Expected=2, Real=0 3. sysctl key kernel.sysrq has a different value than expected in scan profile. Expected=0, Real=16 4. sysctl key net.ipv4.conf.all.forwarding has a different value than expected in scan profile. Expected=0, Real=1 5. sysctl key net.ipv4.conf.all.log_martians contains equal expected and current value (1) 6. sysctl key net.ipv4.conf.all.send_redirects contains equal expected and current value (0) 7. sysctl key net.ipv4.conf.default.accept_redirects contains equal expected and current value (0) 8. sysctl key net.ipv4.conf.default.log_martians contains equal expected and current value (1) 9. sysctl key net.ipv6.conf.all.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1 10. sysctl key net.ipv6.conf.default.accept_redirects has a different value than expected in scan profile. Expected=0, Real=1	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.
31	The AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Release 4 Vuls Exception Request		
32				

Approved Feature Projects

If the program uses only one programming language, in the "Repository" column, just fill in the repo location.

If a project uses multiple programming languages, please list all of them, add a link in "Repository" column for each programming language to show the sample code.

	Project Name	Programming Languages	Repository	SonarQube Enabled	Notes
1	Akraino Blueprint Validation Framework				
2	Akraino Portal Feature Project				
4	Akraino Profiling				
5	Akraino Regional Controller				
6	API Gateway				
7	Backup and Restore (Snappy) Feature Project				
8	Cluster Health & Overload Monitoring Platform (CHOMP) Feature Project				
9	MEC API Framework				
10	Support of OVS-DPDK in Airship				