KUBERNETES STIG
REVISION HISTORY

Version 1, Release 10

26 July 2023

Developed by DISA for the DOD

REVISION HISTORY

Revision Number	Document Revised	Description of Change	Release Date
V1R10	- Kubernetes STIG, V1R9	- CNTR-K8-000270 - Changed check for clarity and consistency. - CNTR-K8-000330 - Revised discussion, check, and fix. The read-only-port option has been deprecated and replaced by the readOnlyPort KubeletConfiguration field. Removed procedure for control plane version worker nodes. - CNTR-K8-000370 - Revised check and fix. The anonymous-auth option has been deprecated and replaced by the "enabled" KubeletAnonymousAuthentication field. Removed procedure for control plane version worker nodes. - CNTR-K8-000380 - Revised check and fix. The authorization-mode option has been deprecated and replaced by the "mode" field in KubeletAuthorization. Removed procedure for control plane version worker nodes. - CNTR-K8-000440 - Revised check and fix to reflect staticPodPath is a valid field for KubeletConfiguration. Removed errant space in title. - CNTR-K8-000450 - Revised check and fix. The kubelet feature-gates option has been deprecated and replaced by the "featureGates" field in KubeletAuthorization. - CNTR-K8-000460 - Revised check and fix. The DynamicKubeletConfig flag was deprecated as of v1.22 and will be removed after v1.25 (end of life 28 October 2023). The kubelet feature-gates option has been deprecated and replaced by the "featureGates" field in KubeletAuthorization. - CNTR-K8-000850 - Revised check and fix as hostname-override is a valid kubelet option. - CNTR-K8-000880 - Changed rule title to refer to KubeletConfiguration file instead of Kubernetes kubelet configuration.	26 July 2023

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- CNTR-K8-000890 - Revised rule title, check, and fix to refer to KubeletConfiguration file instead of Kubernetes kubelet configuration and to look for permissions in the sysconfig and not the manifest directory. - CNTR-K8-000900 - Merged rule title, discussion, check, and fix from CNTR-K8-003250, which is being removed. Added CCI. - CNTR-K8-001300 - Revised discussion, check, and fix. The streaming-connection-idle-timeout option has been deprecated and replaced by the streamingConnectionIdleTimeout KubeletConfiguration field. - CNTR-K8-001410 - Updated discussion, check, and fix to match. - CNTR-K8-001420 - Revised discussion, check, and fix. The client-ca-file option has been deprecated and replaced by the clientCAFile KubeletConfiguration field. Removed redundant API server manifest check. - CNTR-K8-001460 - Revised rule title, discussion, check, and fix. The tls-private-key-file option has been deprecated and replaced by the tlsPrivateKeyFile KubeletConfiguration field. - CNTR-K8-001470 - Revised rule title, discussion, check, and fix. The tls-cert-file option has been deprecated and replaced by the tlsCertFile KubeletConfiguration field. - CNTR-K8-001620 - Revised check and fix. The protect-kernel-defaults option has been deprecated and replaced by the protectKernelDefaults KubeletConfiguration field. - CNTR-K8-001990 - Revised fix for clarity and consistency. - CNTR-K8-002001 - Revised rule title, discussion, check, and fix. The kubelet	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		feature-gates option has been deprecated and replaced by the "featureGates" field in KubeletAuthorization. - CNTR-K8-002620 - Rule number updated due to changes in content management system. - CNTR-K8-002630, CNTR-K8-002640 - Changed severity to CAT I. - CNTR-K8-003160, CNTR-K8-003170 - Revised check and fix. The client-ca-file option has been deprecated and replaced by the clientCAFile KubeletConfiguration field. - CNTR-K8-003190, CNTR-K8-003200 - Changed rule title to refer to KubeConfig file instead of Kubernetes kubelet conf. - CNTR-K8-003250 - Removed this requirement and merged the information into CNTR-K8-000900. - CNTR-K8-003260 - Revised the check and fix commands to be recursive. - CNTR-K8-003330, CNTR-K8-003340 - In check and fix, changed the "find" piped into "xargs" to be recursive into subdirectories. - CNTR-K8-003350 - Removed requirement, which was a duplicate of CNTR-K8-000170.	
V1R9	- Kubernetes STIG, V1R8	- CNTR-K8-003340 - Added sudo to the check. - Rule Key IDs updated due to changes in content management system.	27 April 2023
V1R8	- Kubernetes STIG, V1R7	- CNTR-K8-002700 - Rule number updated due to changes in content management system. - CNTR-K8-003340 - Modified the executable command.	26 January 2023
V1R7	- Kubernetes STIG, V1R6	- CNTR-K8-000150, CNTR-K8-000160, CNTR-K8-000170, CNTR-K8-000180, CNTR-K8-000190, CNTR-K8-000220, CNTR-K8-000270, CNTR-K8-000300, CNTR-K8-000310, CNTR-K8-000320,	27 October 2022

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		CNTR-K8-000340, CNTR-K8-000350, CNTR-K8-000360, CNTR-K8-000400, CNTR-K8-000410, CNTR-K8-000420, CNTR-K8-000430, CNTR-K8-000450, CNTR-K8-000460, CNTR-K8-000470, CNTR-K8-000600, CNTR-K8-000610, CNTR-K8-000700, CNTR-K8-000860, CNTR-K8-000890, CNTR-K8-000900, CNTR-K8-000910, CNTR-K8-000920, CNTR-K8-000930, CNTR-K8-000940, CNTR-K8-000950, CNTR-K8-000960, CNTR-K8-001160, CNTR-K8-001360, CNTR-K8-001400, CNTR-K8-001410, CNTR-K8-001430, CNTR-K8-001440, CNTR-K8-001450, CNTR-K8-001460, CNTR-K8-001470, CNTR-K8-001480, CNTR-K8-001490, CNTR-K8-001500, CNTR-K8-001510, CNTR-K8-001520, CNTR-K8-001530, CNTR-K8-001540, CNTR-K8-001550, CNTR-K8-001620, CNTR-K8-001990, CNTR-K8-002000, CNTR-K8-002010, CNTR-K8-002600, CNTR-K8-002620, CNTR-K8-002630, CNTR-K8-002640, CNTR-K8-002700, CNTR-K8-002720, CNTR-K8-003110, CNTR-K8-003120, CNTR-K8-003130, CNTR-K8-003140, CNTR-K8-003150, CNTR-K8-003160, CNTR-K8-003170, CNTR-K8-003250, CNTR-K8-003260, CNTR-K8-003270, CNTR-K8-003280, CNTR-K8-003290, CNTR-K8-003300, CNTR-K8-003310, CNTR-K8-003320, CNTR-K8-003350 - Removed Master Node and replaced with “Control Plane”. - CNTR-K8-000330, CNTR-K8-000370, CNTR-K8-000380, CNTR-K8-000440, CNTR-K8-000850, CNTR-K8-000880, CNTR-K8-001300, CNTR-K8-001420 - Removed Master Node and replaced with “Control Plane”. Changed check and fix to be accurate and consistent.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- CNTR-K8-002000, CNTR-K8-002010 - Add comments to check that PSP will be deprecated and to use the new Pod Security Admission Controller requirements. - CNTR-K8-002001, CNTR-K8-002011 - PSP has been deprecated; Kubernetes must have Pod Security Admission set.	
V1R6	- Kubernetes STIG, V1R5	- CNTR-K8-001460, CNTR-K8-001470, CNTR-K8-001620 - Corrected typo in Fix: “kuberlet” to “kubelet.”	27 July 2022
V1R5	- Kubernetes STIG, V1R4	- CNTR-K8-001300 - Changed wording of vulnerability discussion and check to consider the default configuration value that already satisfies the requirement. - CNTR-K8-001480 - Changed discussion to reflect correct parameter. - CNTR-K8-002010 - PodSecurity replaced the depreciated PodSecurityPolicy admission controller. - CNTR-K8-003140, CNTR-K8-003160, CNTR-K8-003190, CNTR-K8-003230 - Changed fix from chown to chmod.	27 April 2022
V1R4	- Kubernetes STIG, V1R3	- CNTR-K8-000320, CNTR-K8-000920, CNTR-K8-000940 - Removed deprecated --insecure-port. - CNTR-K8-001450 - Changed control to look for this setting in etcd.yaml. Changed discussion to reflect correct parameter. - CNTR-K8-001490 - Changed control to refer to key-file, not keyfile, and to look for setting in Kubernetes etcd manifest. - CNTR-K8-001500 - Changed control to refer to cert-file, not certfile, and to look for setting in Kubernetes etcd manifest. - CNTR-K8-001510, CNTR-K8-001520, CNTR-K8-001530 - Changed control to look for setting in kube-apiserver.yaml. - CNTR-K8-001540, CNTR-K8-001550 - Changed discussion to reflect correct parameter. - CNTR-K8-002010 - Removed deprecated Docker entry.	27 January 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R3	- Kubernetes STIG, V1R2	- CNTR-K8-000220 - Changed the param name "use-service-account-credentials" not "use-service-account-credential". - CNTR-K8-000890 - Corrected discussion to address least privilege and not "owned by root". - CNTR-K8-001400 - Removed cipher suites using the CHACHA20_POLY1305. Removed extra space before _SHA256. - CNTR-K8-001420, CNTR-K8-001460 - Changed discussion filename to match the check. - CNTR-K8-001490 - Changed control to address etcd param "key-file" rather than "etcd-key-file".	27 October 2021
V1R2	- Kubernetes STIG, V1R1	- CNTR-K8-000180, CNTR-K8-000190 - Modified Vulnerability Discussion to match Check and Fix. - CNTR-K8-001300 - Changed SRGID to SRG-APP-000190-CTR-000500. - CNTR-K8-001480 - Updated control to address peer-client-cert-auth. - CNTR-K8-001500 – Updated control to address certfile instead of etcd-certfile. - CNTR-K8-002620 - Updated text to state basic-auth-file should not be set. - CNTR-K8-002620, CNTR-K8-002630, CNTR-K8-002640 - Changed SRGID to SRG-APP-000439-CTR-001080. - CNTR-K8-003170 - Changed check for file mode for Kubelet to be client-ca-file. - CNTR-K8-003210, CNTR-K8-003220 - Updated Rule Title, Check, and Fix to refer to kubeadm.conf. - CNTR-K8-003250 - Corrected text that incorrectly updates the ownership rather than file mode. - CNTR-K8-003310 - Replaced audit-log-path with audit-log-maxage. - CNTR-K8-003320 – Revised finding statement in Check to reference this is a finding if not set to a valid path.	23 July 2021

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V1R1	- NA	- Initial Release.	13 April 2021