

Release 6: Akraino CVE and KHV Vulnerability Exception Request

1.6.1+dfsg.3-2ubuntu1

Blueprints that have vulnerabilities with a CVSS score ≥ 9.0 and meet the following criteria should submit their information in the chart below to have the vulnerability considered for an exception:

- Running at least the minimum OS version required by the Akraino Security Sub-Committee
 - Ubuntu
 - CentOS
 - Debian
 - Fedora
 - Suse Enterprise Server

Legend

Ubuntu Priority/Score Descriptions

Not Vulnerable	Packages which do not exist in the archive, are not affected by the vulnerability or have a fix applied in the archive.
Pending	A fix has been applied and updated packages are awaiting arrival into the archive. For example, this might be used when wider testing is requested for the updated package.
Unknown	Open vulnerability where the priority is currently unknown and needs to be triaged.
Negligible	Open vulnerability that may be a problem but otherwise does not impose a security risk due to various factors. Examples include when the vulnerability is only theoretical in nature, requires a very special situation, has almost no install base or does no real damage. These typically will not receive security updates unless there is an easy fix and some other issue causes an update.
Low	Open vulnerability that is a problem but does very little damage or is otherwise hard to exploit due to small user base or other factors such as requiring specific environment, uncommon configuration, user assistance, etc. These tend to be included in security updates only when higher priority issues require an update or if many low priority issues have built up.
Medium	Open vulnerability that is a real problem and is exploitable for many users of the affected software. Examples include network daemon denial of service, cross-site scripting and gaining user privileges.
High	Open vulnerability that is a real problem and is exploitable for many users in the default configuration of the affected software. Examples include serious remote denial of service of the system, local root privilege escalations or local data theft.
Critical	Open vulnerability that is a world-burning problem and is exploitable for most Ubuntu users. Examples include remote root privilege escalations or remote data theft.

CVE /KHV #	Blueprint	Blueprint OS/Ver	URL Showing OS Patch Not Available	Contact Name	Contact Email	Comment
CVE-2016-1585	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2016-1585	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-20236	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-20236	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-31870	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-31870	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-31872	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-31872	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-31873	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-31873	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-33574	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-33574	Colin Peters	colin.peters@fujitsu.com	

CVE-2021-45951	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45951	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45952	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45952	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45953	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45953	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45954	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45954	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45955	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45955	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45956	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45956	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-45957	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-45957	Colin Peters	colin.peters@fujitsu.com	
CVE-2022-23218	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2022-23218	Colin Peters	colin.peters@fujitsu.com	
CVE-2022-23219	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2022-23219	Colin Peters	colin.peters@fujitsu.com	
CVE-2016-9180	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2016-9180	Colin Peters	colin.peters@fujitsu.com	
CVE-2021-35942	Smart Data Transaction for CPS	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-35942	Colin Peters	colin.peters@fujitsu.com	[Apr 15 04:10:15] INFO [localhost] Loaded: /vuls/results/2022-04-14T09:51:25Z ... <pre> +-----+-----+-----+-----+-----+-----+-----+-----+ CVE-ID CVSS ATTACK POC ALERT FIXED NVD +-----+-----+-----+-----+-----+-----+-----+ CVE-2021-35942 9.1 AV:N unfixed https://nvd.nist.gov/vuln/detail/CVE-2021-35942 </pre> * The Ubuntu CVE database at https://ubuntu.com/security/cve-2021-35942 reports it is fixed in 20.0 * The version installed on the system is the same as the one specified on the Ubuntu CVE database p <pre> colin@ubuntu20:~\$ dpkg -l libc6 ... / Name Version Architecture Description +++=-----+-----+-----+-----+-----+-----+-----+-----+ ii libc6:amd64 2.31-0ubuntu9.7 amd64 GNU C Library: Shared libraries </pre>
CVE-2016-1585	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2016-1585	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2017-18201	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-18201	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2017-7827	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-7827	Inoue Reo	inoue.reo@fujitsu.com	

CVE-2018-5090	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-5090	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2018-5126	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-5126	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2018-5145	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-5145	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2018-5151	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-5151	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2019-17041	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17041	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2019-17042	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17042	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-31870	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2021-31870	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-31872	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2021-31872	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-31873	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2021-31873	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-39713	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2021-39713	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-23852	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2022-23852	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-23990	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2022-23990	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-25235	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2022-25235	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-25236	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2022-25236	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-25315	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2022-25315	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2016-9180	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2016-9180	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2019-20433	Robot basic architecture based on SSES	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-20433	Inoue Reo	inoue.reo@fujitsu.com	

CVE-2005-2541	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2005-2541	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2014-2830	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2014-2830	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2016-1585	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2016-1585	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2017-17479	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2017-17479	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2017-9117	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2017-9117	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2018-13410	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2018-13410	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2019-1010022	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2019-1010022	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2019-8341	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2019-8341	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2020-27619	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2020-27619	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-29462	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-29462	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-29921	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-29921	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-30473	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-30473	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-30474	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-30474	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-30475	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-30475	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-30498	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-30498	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-30499	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-30499	Inoue Reo	inoue.reo@fujitsu.com	

CVE-2021-42377	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-42377	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45951	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45951	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45952	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45952	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45953	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45953	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45954	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45954	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45955	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45955	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-45956	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-45956	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-23303	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2022-23303	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2022-23304	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2022-23304	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-4048	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-4048	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-43400	Robot basic architecture based on SSES	Raspberry Pi OS(Debian 11)	https://security-tracker.debian.org/tracker/CVE-2021-43400	Inoue Reo	inoue.reo@fujitsu.com	
CVE-2021-33574	ICN	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-33574	Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com	
CVE-2019-19814	ICN	Ubuntu 20.04	https://ubuntu.com/security/CVE-2019-19814	Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com	
CVE-2021-35942	ICN	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-35942	Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com	Vendor status is "Released" and ICN is using the referenced glibc version, however vuls is still reporting libc6 output: <pre> Distributor ID: Ubuntu Description: Ubuntu 20.04.4 LTS Release: 20.04 Codename: focal No LSB modules are available. Desired=Unknown/Install/Remove/Purge/Hold Status=Not/Inst/Conf-files/Unpacked/half-dfn/Inst / Err?=(none)/Reinst-required (Status,Err: uppercase=bad) / Name Version Architecture Description ++-+-----+-----+-----+-----+ ii libc6:amd64 2.31-0ubuntu9.7 amd64 GNU C Library: Shared libraries </pre>

KHV044	ELIOT - IOTGateway				khemendra.kumar@huawei.com	KHV044 - Privileged Container Minimize the use of privileged containers. Use Pod Security Policies to enforce using privileged: false p Calico pod is running in privileged Mode. Exception Reason: Calico deployed by manifest file, can not be set to non privileged mode. Here is a link regarding the Calico Privilege Mode issue. "Replace Kubernetes privileged=true with more precise permissions" It seems after long time they have make option to disable recently but only if calico deployed with Cal And there is a doc about non-privileged use of running Calico node for operator only. In our ELIOT IOT Gateway BP, it is deployed by calico.yaml file. and with manifest file, they don't support to disable it. So due to Calico limitation, and our ustream project dependency on calico.yaml manifest file, we can no IN future, we can ask the upstream EdgeGallery community to use calico operator for deployment and i be able to fix in our BPs,
KHV044	EALTEdge - Enterprise application on 5G light weight telco edge				khemendra.kumar@huawei.com	KHV044 - Privileged Container Minimize the use of privileged containers. Use Pod Security Policies to enforce using privileged: false p Calico pod is running in privileged Mode. Exception Reason: Calico deployed by manifest file, can not be set to non privileged mode. Here is a link regarding the Calico Privilege Mode issue. "Replace Kubernetes privileged=true with more precise permissions" It seems after long time they have make option to disable recently but only if calico deployed with Cal And there is a doc about non-privileged use of running Calico node for operator only. In our EALTEdge BP, it is deployed by calico.yaml file. and with manifest file, they don't support to disable it. So due to Calico limitation, and our ustream project dependency on calico.yaml manifest file, we can no IN future, we can ask the upstream EdgeGallery community to use calico operator for deployment and i be able to fix in our BPs,
CAP_NET_RAW	EALTEdge - Enterprise application on 5G light weight telco edge				khemendra.kumar@huawei.com	CAP_NET_RAW Enabled CAP_NET_RAW is used to open a raw socket and is used by ping. If this is not required CAP_NET_RA https://www.suse.com/c/demystifying-containers-part-iv-container-security/ For this BP, execption is approved in last release. plz refer last release exeception list Release 5 Blueprint Scanning Status
CVE-2017-12194	IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Ubuntu 18.04	https://ubuntu.com/security/cve-2017-12194	Ysemi	rd-sw@ysemi.cn	lsb_release -a : No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 18.04.6 LTS Release: 18.04 Codename: bionic dpkg -l libspice-server1: Desired=Unknown/Install/Remove/Purge/Hold Status=Not/Inst/Conf-files/Unpacked/half-conf/Half-inst/trig-aWait/Trig-pend / Err?=(none)/Reinst-required (Status,Err: uppercase=bad) / Name Version Architecture Description +++===== ===== ii libspice-server1:arm64 0.14.0-1ubuntu2.1 arm64 Implements the server side of the SPICE protocol
CVE-2018-12892	IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Ubuntu 18.04	https://ubuntu.com/security/cve-2018-12892	Ysemi	rd-sw@ysemi.cn	lsb_release -a : No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 18.04.6 LTS Release: 18.04 Codename: bionic sudo dpkg -l grep xen ii libxen-4.9:arm64 4.9.2-0ubuntu1 arm64 Public libs for Xen ii libxen-dev:arm64 4.9.2-0ubuntu1 arm64 Public headers and libs for Xen ii libxenstore3.0:arm64 4.9.2-0ubuntu1 arm64 Xenstore communications library for Xen

CVE-2019-17113	IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Ubuntu 18.04	https://ubuntu.com/security/cve-2019-17113	Ysemi	rd-sw@ysemi.cn	lsb_release -a : No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 18.04.6 LTS Release: 18.04 Codename: bionic sudo dpkg -I libopenmpt-modplug1 Desired=Unknown/Install/Remove/Purge/Hold Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend / Err?=(none)/Reinst-required (Status,Err: uppercase=bad) / Name Version Architecture Description +++----- ===== ===== ii libopenmpt-modplug1:arm64 0.3.6-1 arm64 module music library based on OpenMPT -- modplug core
CVE-2019-19948	IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Ubuntu 18.04	https://ubuntu.com/security/cve-2019-19948	Ysemi	rd-sw@ysemi.cn	lsb_release -a : No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 18.04.6 LTS Release: 18.04 Codename: bionic dpkg -I grep magick ii imagemagick-6-common 8:6.9.7.4+dfsg-16ubuntu6.12 all image manipulation programs -- infrastructure ii libmagickcore-6.q16-3:arm64 8:6.9.7.4+dfsg-16ubuntu6.12 arm64 low-level image manipulation library ii libmagickwand-6.q16-3:arm64 8:6.9.7.4+dfsg-16ubuntu6.12 arm64 image manipulation library -- quantum magick -version: Version: ImageMagick 7.1.0-33 beta Q16-HDRI aarch64 a2b2c088f:20220430 https://imagemagick.org Copyright: (C) 1999 ImageMagick Studio LLC License: https://imagemagick.org/script/license.php Features: Cipher DPC HDRI OpenMP(4.5) Delegates (built-in): fontconfig freetype lzma pangocairo png x xml zlib Compiler: gcc (7.5)
CVE-2019-19949	IEC Type 3: Android cloud native applications on Arm servers in edge for Integrated Edge Cloud (IEC) Blueprint Family	Ubuntu 18.04	https://ubuntu.com/security/cve-2019-19949	Ysemi	rd-sw@ysemi.cn	lsb_release -a : No LSB modules are available. Distributor ID: Ubuntu Description: Ubuntu 18.04.6 LTS Release: 18.04 Codename: bionic dpkg -I grep magick ii imagemagick-6-common 8:6.9.7.4+dfsg-16ubuntu6.12 all image manipulation programs -- infrastructure ii libmagickcore-6.q16-3:arm64 8:6.9.7.4+dfsg-16ubuntu6.12 arm64 low-level image manipulation library ii libmagickwand-6.q16-3:arm64 8:6.9.7.4+dfsg-16ubuntu6.12 arm64 image manipulation library -- quantum magick -version: Version: ImageMagick 7.1.0-33 beta Q16-HDRI aarch64 a2b2c088f:20220430 https://imagemagick.org Copyright: (C) 1999 ImageMagick Studio LLC License: https://imagemagick.org/script/license.php Features: Cipher DPC HDRI OpenMP(4.5) Delegates (built-in): fontconfig freetype lzma pangocairo png x xml zlib Compiler: gcc (7.5)
KHV043	EALTEdge - Enterprise application on 5G light weight telco edge				khemendra.kumar@huawei.com	Issue: KHV043 - Cluster Health Disclosure Issue description: The kubelet is leaking it's health information, which may contain sensitive information through the /healthz endpoint. This endpoint is exposed as part of the kubelet's handlers. Suggested Remediation: Disable --enable-debugging-handlers kubelet flag. Exception Reason: With current analysis, the above solution to fix this issue is causing impact on basic commands Like after disabling this flag, we can not do logs and exec cmd for any container in the cluster, we check their workload. if disable kubelet debug flags, then it is not possible to see the logs of any pods Or do exec cmds. So after disabling this flag, kubectl "logs" & "exec" cmd is not working. Currently this issue can not be fixed with the provided solution. We request an exception for this issue for release 6.

KHV043	ELIOT - IOT Gateway			khemendra.kumar@huawei.com	Issue: KHV043 - Cluster Health Disclosure Issue description: The kubelet is leaking it's health information, which may contain sensitive information through the /healthz endpoint. This endpoint is exposed as part of the kubelet handlers. Suggested Remediation: Disable --enable-debugging-handlers kubelet flag. Exception Reason: With current analysis, the above solution to fix this issue is causing impact on basic commands Like after disabling this flag, we can not do logs and exec cmd for any container in the cluster, we can't check their workload. if disable kubelet debug flags, then it is not possible to see the logs of any pods Or do exec cmds. So after disabling this flag, kubectl "logs" & "exec" cmd is not working. Currently this issue can not be fixed with the provided solution. We request an exception for this issue for release 6.
--------	---------------------	--	--	--	---