Akraino CVE 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

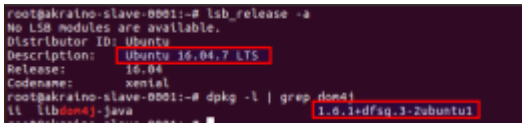
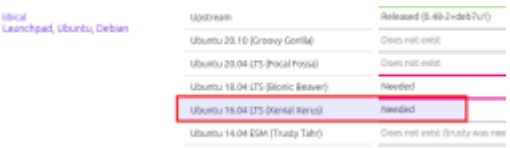
Legend

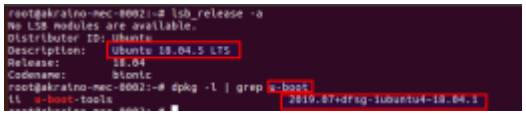
Ubuntu Priority/Score Descriptions

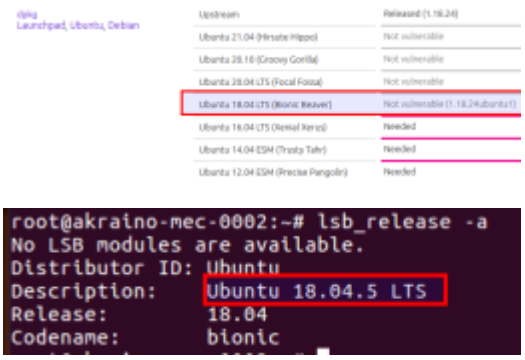
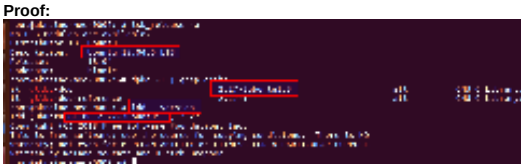
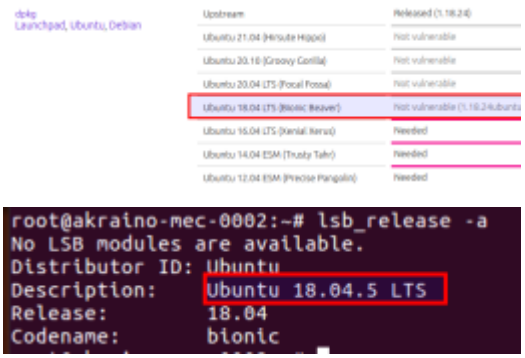
Not Vulnerable	Packages which do not exist in the archive, are not affected by the vulnerability or have a fix applied in the archive.
Pending	A fix has been applied and updated packages are awaiting arrival into the archive. For example, this might be used when wider testing is requested for the updated 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 #	Blueprint	Blueprint OS/Ver	URL Showing OS Patch Not Available	Contact Name	Contact Email	Comment	Vendor CVSS Score	Vendor Patch Available
CVE-2016-1585	KubeEdge Edge Service Blueprint	Ubuntu 20.04	https://ubuntu.com/security/CVE-2016-1585	Yin Ding Hao Xu	yin.ding@futurewei.com		Medium	No
CVE-2017-8283	KubeEdge Edge Service Blueprint	Ubuntu 20.04	https://ubuntu.com/security/CVE-2017-8283	Yin Ding Hao Xu	yin.ding@futurewei.com		Negligible	No
CVE-2018-20839	KubeEdge Edge Service Blueprint	Ubuntu 20.04	https://ubuntu.com/security/CVE-2018-20839	Yin Ding Hao Xu	yin.ding@futurewei.com		Medium	No
CVE-2019-19814	KubeEdge Edge Service Blueprint	Ubuntu 20.04	https://ubuntu.com/security/CVE-2019-19814	Yin Ding Hao Xu	yin.ding@futurewei.com		Low	No
CVE-2013-1910	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2013-1910	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No
CVE-2016-1585	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-1585	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No

CVE-2016-5407	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-5407	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7944	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7944	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7947	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7947	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7948	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7948	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7949	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7949	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7950	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7950	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-7951	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-7951	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-8735	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-8735	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	Released (6.0.45+dfsg-1ubuntu0.1) **Explanation:** We are using same version of integrated OS package as mentioned as re ubuntu for Package dfsg. But still issue thrown. It is not an issue from our side. This issue is with Vuls or Ubuntu. **Proof:** 
CVE-2017-10684	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-10684	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-10685	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-10685	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-12424	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-12424	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-12562	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-12562	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-15088	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-15088	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	No
CVE-2017-18342	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-18342	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-7614	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-7614	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-8283	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-8283	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	No
CVE-2018-12699	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2018-12699	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2018-20839	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2018-20839	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No

CVE-2019-17041	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-17041	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-17042	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-17042	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-17571	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-17571	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No
CVE-2020-10683	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2020-10683	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	Released (1.6.1+dfsg.3-2ubuntu1.1) **Explanation:** This is OS integrated package and we are using 1.6.1+dfsg.3-2ubuntu1 s updated latest release version. This is an issue with Vuls / Ubuntu not fro **Proof:** 
CVE-2020-1938	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2020-1938	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-19814	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-19814	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-19816	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-19816	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	Package: linux For ubuntu 16.04, status is Needed. Package not available for ubuntu 16.04 
CVE-2016-9584	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-9584	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	Package: libical For Ubuntu 16.04, status is Needed for Libical Package. Package not available for ubuntu 16.04 
CVE-2017-5209	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-5209	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	No
CVE-2017-5545	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-5545	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	No
CVE-2017-6969	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-6969	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-7226	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-7226	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-8872	ELIOT IOTGateway	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-8872	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No

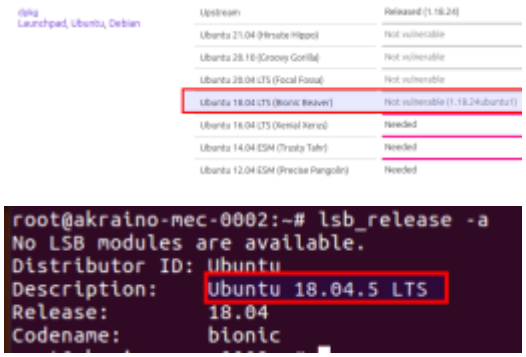
CVE-2019-15505	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-15505	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 8.0	No
CVE-2014-9939	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2014-9939	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low 1.2	No
CVE-2017-12652	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2017-12652	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low 3.7	There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS **Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2018-16428	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2018-16428	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low 5.1	**No** There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS
CVE-2019-11068	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-11068	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 6.3	There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS **Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-12450	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-12450	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 6.6	There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS **Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-12900	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-12900	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low 4.0	**No** There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS
CVE-2019-9169	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-9169	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 6.5	**No (Will not fix)** There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS
CVE-2018-20836	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2018-20836	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 7.0	There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS **Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-2201	ELIOT uCPE	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-2201	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Moderate 7.8	**No (Will not fix)** There is no proper documents from CENTOS for unfixed vulnerabilities. cannot compare/refer RHEL 7 docs with CENTOS 7.8 since, RHEL is cor different OS
CVE-2018-18439	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-18439	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	Not vulnerable (2019.07+dfsg-1ubuntu4~18.04.1) **Screenshot:** 
CVE-2020-8432	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2020-8432	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2016-1585	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2016-1585	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No
CVE-2017-18342	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-18342	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No

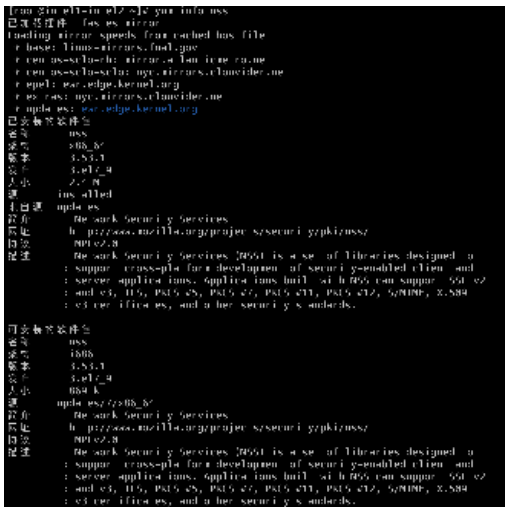
CVE-2017-8283	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-8283	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Negligible	18.04 Not vulnerable 1.18..24ubuntu1 
CVE-2018-11236	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-11236	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	glibc: Fix 2.27-3ubuntu1.2 **Explanation:** We are using same version of integrated OS package updated as mentio released by ubuntu for Package glibc. But still issue thrown. It is **not an issue from our side**. This **issue is with Vuls or Ubuntu.** **Proof:** 
CVE-2018-20839	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-20839	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	No
CVE-2019-11059	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-11059	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	**18.04 LTS**: **Not Vulnerable** 2019.07+dfsg-1ubuntu4~18.04.1 **Screenshots:** 
CVE-2019-14192	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14192	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14193	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14193	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14194	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14194	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14195	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14195	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14196	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14196	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No

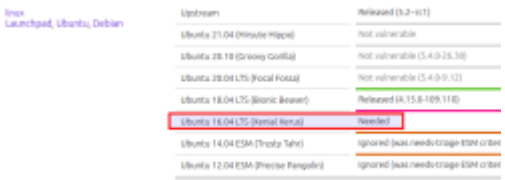
CVE-2019-14198	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14198	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14199	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14199	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14200	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14200	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14201	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14201	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14202	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14202	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14203	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14203	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-14204	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14204	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-9169	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-9169	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-10220	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-10220	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Medium	linux Minimum 4.15.0-88.88 **Explanation:** We are using the latest patch of linux kernel. Since we are using updatec patch. Still issues thrown. This is an issue from Vuls / Ubuntu not from our side **Screenshot**:  4.15.0-118-generic installed
CVE-2019-19814	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-19814	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2019-19816	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-19816	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	linux 4.15.0-88.88 minimum required **Explanation:** We are **using the latest patch of linux kernel**. Eventhough we are usin patch, Still issues thrown. This is an issue from Vuls / Ubuntu not from our side **Screenshot:**  4.15.0-118-generic installed
CVE-2019-14197	EALT-Edge	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14197	Srinivasan Selvam	srinivasanselvam2014@gmail.com		Low	No
CVE-2017-12652	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2017-12652	zifan wu	wuzifan0817@gmail.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Low 3.7	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**

CVE-2019-11068	The AI Edge: Federated ML application at the edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-11068	zifan wu	wuzifan0817@gmail.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Low 6.3	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-12450	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12450	zifan wu	wuzifan0817@gmail.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Moderate 6.6	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-12900	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12900	zifan wu	wuzifan0817@gmail.com	We need exception request for this CVE as it is not yet fixed for 7.X version	LOW 4.0	No
CVE-2018-20836	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2018-20836	zifan wu	wuzifan0817@gmail.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Moderate 7.0	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-8506	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8506	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 6.3	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8535	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8535	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 6.3	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8536	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8536	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 6.3	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8544	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8544	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 6.3	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8669	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8669	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8672	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8672	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8676	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8676	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**

CVE-2019-8684	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8684	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8688	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8688	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8689	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8689	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8814	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8814	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8815	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8815	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-8816	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8816	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2020-3868	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-3868	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2020-3895	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-3895	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2020-3897	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-3897	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2020-3899	The AI Edge: Federated ML application at edge	Centos7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-3899	zifan wu	wuzifan0817@gmail.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 8.8	**webkitgtk4 - Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020** **webkitgtk3 - Will not fix**
CVE-2019-2201	The AI Edge: School /Education Video Security Monitoring	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-2201	@Hechun Zhang	zhanghechun@baidu.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 7.8	No

CVE-2019-12900	The AI Edge: School /Education Video Security Monitoring	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-12900	@Hechun Zhang	zhanghechun@baidu.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Low 4.0	No
CVE-2019-18218	The AI Edge: School /Education Video Security Monitoring	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-18218	@Hechun Zhang	zhanghechun@baidu.com	This is a bug for the host machine, not for the runtime environment for the Blueprint.	Moderate 9.8	No
CVE-2018-16428	The AI Edge: School /Education Video Security Monitoring	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2018-16428	@Hechun Zhang	zhanghechun@baidu.com		Low 5.1	No
CVE-2019-14889	The AI Edge: School /Education Video Security Monitoring	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-14889	@Hechun Zhang	zhanghechun@baidu.com		Low	Package: libssh2 not affected Package: libssh fixed 11/3/2020 in RHSA-2020:4545
CVE-2016-1585	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2016-1585	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Medium	No
CVE-2017-18342	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-18342	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No
CVE-2017-8283	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-8283	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Negligible	18.04 Not vulnerable 1.18..24ubuntu1 
CVE-2018-20839	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-20839	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Medium	No
CVE-2019-19814	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-19814	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No
CVE-2019-17041	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17041	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No
CVE-2019-17042	ICN	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17042	@Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No
CVE-2021-33574	ICN	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-33574	Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No
CVE-2019-19814	ICN	Ubuntu 20.04	https://ubuntu.com/security/CVE-2019-19814	Kuralamudhan Ramakrishnan	kuralamudhan.ramakrishnan@intel.com		Low	No

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 this	Low	Yes
CVE-2017-12652	REC	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2017-12652	Paul Carver	pcarver@att.com		Low 3.7	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-11068	REC	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-11068	Paul Carver	pcarver@att.com		Moderate 6.8	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-12450	REC	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-12450	Paul Carver	pcarver@att.com		Moderate 6.6	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-17006	REC	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-12450	Paul Carver	pcarver@att.com		Moderate 8.1	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-5482	REC	CentOS 7.8	https://access.redhat.com/security/cve/CVE-2019-12450	Paul Carver	pcarver@att.com		Moderate 6.3	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2017-12652	Connected Vehicle Blueprint (CVB)	CentOS 7.8	https://nvd.nist.gov/vuln/detail/CVE-2017-12652	abhimanyu	abhimanyu@parserlabs.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Low 3.7	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-5482	Connected Vehicle Blueprint (CVB)	CentOS 7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-5482	abhimanyu	abhimanyu@parserlabs.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Moderate 6.3	**Fixed in RHEL 7 But not in CentOS 7.8 as of 9/29/2020**
CVE-2019-17006	IEC Type4-AR/VR oriented Edge Stack	CentOS 7.9	https://access.redhat.com/security/cve/CVE-2019-17006	Eaton Zhang	eatonzhang@tencent.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Moderate 8.1	**It is cause by nss before 3.46, but the version is already 3.53.1. But s thrown.** **It is not an issue from our side. This issue is with Vuls or CentOS.** 
CVE-2017-12652	5G MEC /Slice System to Support Cloud Gaming, HD Video and Live Broadcasting Blueprint	CentOS 7.6	https://access.redhat.com/security/cve/CVE-2017-12652	Zigeng Fu	eaganfu@tencent.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Low 3.7	No

CVE-2019-5482	5G MEC /Slice System to Support Cloud Gaming, HD Video and Live Broadcasting Blueprint	CentOS 7.6	https://access.redhat.com/security/cve/CVE-2019-5482	Zigeng Fu	eaganfu@tencent.com	We need exception request for this CVE as it is not yet fixed for 7.X version	Moderate 6.3	No
CVE-2016-1585	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2016-1585	Sukhdev Kapur	sukhdevkapur@gmail.com		Medium	No
CVE-2017-10684	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-10684	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-10685	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-10685	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-12424	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-12424	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-15088	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-15088	Sukhdev Kapur	sukhdevkapur@gmail.com		Negligible	No
CVE-2017-18342	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-18342	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-7614	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-7614	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-8283	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-8283	Sukhdev Kapur	sukhdevkapur@gmail.com		Negligible	No
CVE-2018-12699	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2018-12699	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2018-20839	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2018-20839	Sukhdev Kapur	sukhdevkapur@gmail.com		Medium	No
CVE-2019-17041	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-17041	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2019-17042	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-17042	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2019-19814	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-19814	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2019-19816	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-19816	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	Package: linux For ubuntu 16.04, status is Needed. Package not available for ubuntu 16.04 
CVE-2017-6969	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-6969	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2017-7226	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-7226	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No

CVE-2017-8872	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2017-8872	Sukhdev Kapur	sukhdevkapur@gmail.com		Low	No
CVE-2019-13224	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-13224	Sukhdev Kapur	sukhdevkapur@gmail.com		Medium	No
CVE-2019-19012	Network Cloud and Tungsten Fabric	Ubuntu 16.04	https://ubuntu.com/security/CVE-2019-19012	Sukhdev Kapur	sukhdevkapur@gmail.com		Medium	No
CVE-2017-8283	PCEI	Ubuntu 18.04	https://ubuntu.com/security/cve-2017-8283	Oleg Berzin	oberzin@equinix.com		Negligible	No
CVE-2019-19814	PCEI	Ubuntu 18.04	https://ubuntu.com/security/cve-2019-19814	Oleg Berzin	oberzin@equinix.com		Low	No
CVE-2016-1585	PCEI	Ubuntu 18.04	https://ubuntu.com/security/CVE-2016-1585	Oleg Berzin	oberzin@equinix.com		Medium	No
CVE-2017-18342	PCEI	Ubuntu 18.04	https://ubuntu.com/security/CVE-2017-18342	Oleg Berzin	oberzin@equinix.com		Low	No
CVE-2018-20839	PCEI	Ubuntu 18.04	https://ubuntu.com/security/CVE-2018-20839	Oleg Berzin	oberzin@equinix.com		Medium	No
CVE-2019-17041	PCEI	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17041	Oleg Berzin	oberzin@equinix.com		Low	No
CVE-2019-17042	PCEI	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17042	Oleg Berzin	oberzin@equinix.com		Low	No
CVE-2016-9085	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2016-9085	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2017-18201	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2017-18201	hanyu ding	dinghanyu@chinamobile.com		Medium	No
CVE-2017-9525	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2017-9525	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-10160	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2019-10160	hanyu ding	dinghanyu@chinamobile.com		low	No
CVE-2019-18276	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2019-18276	hanyu ding	dinghanyu@chinamobile.com		low	No
CVE-2020-27619	IEC TYPE3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2020-27619	hanyu ding	dinghanyu@chinamobile.com		low	No
CVE-2021-3177	IEC Type3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2021-3177	hanyu ding	dinghanyu@chinamobile.com		low	No
CVE-2016-9180	IEC Type3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2016-9180	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-13103	IEC Type3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2019-13103	hanyu ding	dinghanyu@chinamobile.com		low	No
CVE-2019-9948	IEC Type3	Ubuntu 18.04	https://nvd.nist.gov/vuln/detail/CVE-2019-9948	hanyu ding	dinghanyu@chinamobile.com		low	No

CVE-2019-14192	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14192	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14193	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14193	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14194	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14194	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14195	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14195	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14196	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14196	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14198	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14198	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14199	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14199	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14200	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14200	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14201	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14201	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14202	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14202	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14203	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14203	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-17041	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17041	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-17042	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-17042	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2020-8432	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2020-8432	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14197	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14197	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2019-14204	IEC Type3	Ubuntu 18.04	https://ubuntu.com/security/CVE-2019-14204	hanyu ding	dinghanyu@chinamobile.com		Low	No
CVE-2018-10103	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2018-10103	yihui wang	wangyihui@chinamobile.com		Moderate	Package: tcpdump Description: RHSA-2020:4760 Fixed Date: 11/3/20
CVE-2018-10105	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2018-10105	yihui wang	wangyihui@chinamobile.com		Moderate	Package: tcpdump Description: RHSA-2020:4760 Fixed Date: 11/3/20
CVE-2018-19325	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2018-14466 see note for CVE #	yihui wang	wangyihui@chinamobile.com		Low	Per https://nvd.nist.gov/vuln/detail/CVE-2018-19325 this CVE is a duplica 2018-14466, this later CVE should be the only one referenced moving for Package: tcpdump Description: RHSA-2020:4760 Fixed Date: 11/3/20

CVE-2019-12900	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-12900	yihui wang	wangyihui@chinamobile.com		Low	No; will not fix
CVE-2019-16746	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-16746	yihui wang	wangyihui@chinamobile.com		Moderate	No; will not fix
CVE-2019-14889	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-14889	yihui wang	wangyihui@chinamobile.com		Low	Package: libssh2 not affected Package: libssh fixed 11/3/2020 in RHSA-2020:4545
CVE-2019-17544	IEC Type 5	CentOS 8.2	https://access.redhat.com/security/cve/CVE-2019-17544	yihui wang	wangyihui@chinamobile.com		Low	No; will not fix
CVE-2019-18604	AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Ubuntu 20.04	https://ubuntu.com/security/CVE-2019-18604	Hechun Zhang Hao Zhongwang	zhanghechun@baidu.com		Low	No
CVE-2020-14343	AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Ubuntu 20.04	https://ubuntu.com/security/CVE-2020-14343	Hechun Zhang Hao Zhongwang	zhanghechun@baidu.com		Medium	No
CVE-2020-27619	AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Ubuntu 20.04	https://ubuntu.com/security/CVE-2020-27619	Hechun Zhang Hao Zhongwang	zhanghechun@baidu.com		Low	Specify version of Python being used. Python 3.8 has a patch, other don't or not vulnerable on Ubuntu 20.04
CVE-2021-3177	AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Ubuntu 20.04	https://ubuntu.com/security/CVE-2021-3177	Hechun Zhang Hao Zhongwang	zhanghechun@baidu.com		Medium	Specify version of Python being used. Python 3.8 has a patch, other don't or not vulnerable on Ubuntu 20.04
CVE-2016-9180	AI Edge: Intelligent Vehicle-Infrastructure Cooperation System(I-VICS)	Ubuntu 20.04	https://ubuntu.com/security/CVE-2016-9180	Hechun Zhang Hao Zhongwang	zhanghechun@baidu.com		Low	No