Maturity Blueprints: Akraino CVE and KHV Vulnerability Exception Request

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

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	Vendor CVSS Score	Vendor Patch Available	Exception Status
CVE-2022-25315	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-25315	jin peng	jinpeng@soconoc.ai	`expat fixed package is available. Please update the package or remove it if not needed.`	`9.8`	Yes, 2.2.5-3	Not Approved
CVE-2022-25236	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-25236	jin peng	jinpeng@soconoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	`9.8`	Yes, 2.2.5-3	Not Approved
CVE-2022-25235	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-25235	jin peng	jinpeng@soconoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	`9.8`	Yes, 2.2.5-3	Not Approved
CVE-2022-23852	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-23852	jin peng	jinpeng@soconoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	`9.8`	Yes, 2.2.5-3	Not Approved
CVE-2022-22824	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-22824	jin peng	jinpeng@soconoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	`9.8`	Yes, 2.2.5-3	Not Approved

CVE-2022-22823	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-22823	jin peng	jinpeng@socnoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	9.8	Yes, 2.2.5-3	Not Approved
CVE-2022-22822	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2022-22822	jin peng	jinpeng@socnoc.ai	expat fixed package is available. Please update the package or remove it if not needed.	9.8	Yes, 2.2.5-3	Not Approved
CVE-2015-4042	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2015-4042	jin peng	jinpeng@socnoc.ai		9.8	No	Approved
CVE-2014-9939	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2014-9939	jin peng	jinpeng@socnoc.ai		9.8	No	Approved
CVE-2021-43527	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu18.04	https://ubuntu.com/security/CVE-2021-43527	jin peng	jinpeng@socnoc.ai	nss fixed packages is available. Please update the package or remove it if not needed.	10.0	Yes 2:3.35-2	Not Approved
CVE-2022-0318	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu20.04	https://ubuntu.com/security/CVE-2022-0318	jin peng	jinpeng@socnoc.ai		9.8	No	Approved
CVE-2022-30767	Release 6 Documentation for IEC Type 5: Composable Integrated Edge Cloud (IEC) Server Blueprint Family	ubuntu20.04	https://ubuntu.com/security/CVE-2022-30767	jin peng	jinpeng@socnoc.ai		9.8	No	Approved