

docker.io/velotixai/redis:349028b-11.03.1326-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	

docker.io/velotixai/discovery:b3e1d0b-11.05.0828-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	
jar	
No Vulnerabilities found	
No Misconfigurations found	
gobinary	
No Vulnerabilities found	
No Misconfigurations found	

docker.io/velotixai/kafka:c879fa4-11.05.0823-main (wolfi 20230201) - Trivy Report

wolfi					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
libcrypto3	CVE-2024-9143	LOW	3.3.2-r0	3.3.2-r2	<a href="https://access.redhat.com/security/cve/CVE-2024-9143">https://access.redhat.com/security/cve/CVE-2024-9143</a>
No Misconfigurations found					

docker.io/velotixai/mlscoring:bae5fc0-11.05.0414-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	
python-pkg	
No Vulnerabilities found	
No Misconfigurations found	

docker.io/velotixai/mljobscheduler:bae5fc0-11.05.0414-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	
python-pkg	
No Vulnerabilities found	
No Misconfigurations found	

docker.io/velotixai/search:b3e1d0b-11.05.0828-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	
jar	
No Vulnerabilities found	
No Misconfigurations found	
gobinary	
No Vulnerabilities found	
No Misconfigurations found	

docker.io/velotixai/fluent-bit:271c283-09.08.0635-main (wolfi 20230201) - Trivy Report

wolfi					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
libcrypto3	CVE-2024-9143	LOW	3.3.2-r0	3.3.2-r2	<a href="https://access.redhat.com/security/cve/CVE-2024-9143">https://access.redhat.com/security/cve/CVE-2024-9143</a>
libssl3	CVE-2024-9143	LOW	3.3.2-r0	3.3.2-r2	<a href="https://access.redhat.com/security/cve/CVE-2024-9143">https://access.redhat.com/security/cve/CVE-2024-9143</a>
No Misconfigurations found					

docker.io/velotixai/fe:1538e3e-11.05.0853-main (wolfi 20230201) - Trivy Report

wolfi	
No Vulnerabilities found	
No Misconfigurations found	
jar	
No Vulnerabilities found	
No Misconfigurations found	
python-pkg	
No Vulnerabilities found	
No Misconfigurations found	
gobinary	

No Vulnerabilities found
No Misconfigurations found

docker.io/velotixai/mlinterface:b4a4b09-11.03.1323-main (wolfi 20230201) - Trivy Report

wolfi					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
python-3.10	CVE-2024-9287	MEDIUM	3.10.15-r2	3.10.15-r3	<a href="https://access.redhat.com/security/cve/CVE-2024-9287">https://access.redhat.com/security/cve/CVE-2024-9287</a>
python-3.10-base	CVE-2024-9287	MEDIUM	3.10.15-r2	3.10.15-r3	<a href="https://access.redhat.com/security/cve/CVE-2024-9287">https://access.redhat.com/security/cve/CVE-2024-9287</a>
No Misconfigurations found					
python-pkg					
No Vulnerabilities found					
No Misconfigurations found					

docker.io/velotixai/superset:9f8e129-11.03.1327-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
node-pkg					
No Vulnerabilities found					
No Misconfigurations found					
python-pkg					
No Vulnerabilities found					
No Misconfigurations found					
gobinary					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
stdlib	CVE-2024-24790	CRITICAL	1.22.1	1.21.11, 1.22.4	<a href="http://www.openwall.com/lists/oss-security/2024/07/01">http://www.openwall.com/lists/oss-security/2024/07/01</a>
stdlib	CVE-2023-45288	HIGH	1.22.1	1.21.9, 1.22.2	<a href="http://www.openwall.com/lists/oss-security/2024/07/01">http://www.openwall.com/lists/oss-security/2024/07/01</a>
stdlib	CVE-2024-24788	HIGH	1.22.1	1.22.3	<a href="http://www.openwall.com/lists/oss-security/2024/07/01">http://www.openwall.com/lists/oss-security/2024/07/01</a>
stdlib	CVE-2024-34156	HIGH	1.22.1	1.22.7, 1.23.1	<a href="https://access.redhat.com/errata/RHSA-2024-8111">https://access.redhat.com/errata/RHSA-2024-8111</a>
stdlib	CVE-2024-24789	MEDIUM	1.22.1	1.21.11, 1.22.4	<a href="http://www.openwall.com/lists/oss-security/2024/07/01">http://www.openwall.com/lists/oss-security/2024/07/01</a>
stdlib	CVE-2024-24791	MEDIUM	1.22.1	1.21.12, 1.22.5	<a href="https://access.redhat.com/errata/RHSA-2024-6911">https://access.redhat.com/errata/RHSA-2024-6911</a>
stdlib	CVE-2024-34155	MEDIUM	1.22.1	1.22.7, 1.23.1	<a href="https://access.redhat.com/errata/RHSA-2024-8111">https://access.redhat.com/errata/RHSA-2024-8111</a>
stdlib	CVE-2024-34158	MEDIUM	1.22.1	1.22.7, 1.23.1	<a href="https://access.redhat.com/errata/RHSA-2024-8111">https://access.redhat.com/errata/RHSA-2024-8111</a>
No Misconfigurations found					

docker.io/velotixai/tika:3d11996-10.28.1540-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
jar					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
org.eclipse.jetty:jetty-http	CVE-2024-6763	LOW	11.0.24	12.0.12	<a href="https://access.redhat.com/security/cve/CVE-2024-6763">https://access.redhat.com/security/cve/CVE-2024-6763</a>
No Misconfigurations found					

docker.io/velotixai/presidio:a977dd0-11.03.1332-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
python-pkg					
No Vulnerabilities found					
No Misconfigurations found					

docker.io/velotixai/client:088c979-11.05.0754-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					

docker.io/velotixai/elasticsearch:9f0f909-10.28.1541-main (ubuntu 20.04) - Trivy Report

ubuntu					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
coreutils	CVE-2016-2781	LOW	8.30-3ubuntu2		<a href="http://seclists.org/oss-sec/2016/q1/452">http://seclists.org/oss-sec/2016/q1/452</a> <a href="http://www.openwall.com/lists/oss-security/2016/01/06">http://www.openwall.com/lists/oss-security/2016/01/06</a>
gpgv	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		<a href="https://access.redhat.com/security/cve/CVE-2022-3219">https://access.redhat.com/security/cve/CVE-2022-3219</a>
libc-bin	CVE-2016-20013	LOW	2.31-0ubuntu9.16		<a href="https://akkadia.org/drepper/SHA-crypt.txt">https://akkadia.org/drepper/SHA-crypt.txt</a> <a href="https://www.openwall.com/lists/oss-security/2016/01/06">https://www.openwall.com/lists/oss-security/2016/01/06</a>
libc6	CVE-2016-20013	LOW	2.31-0ubuntu9.16		<a href="https://akkadia.org/drepper/SHA-crypt.txt">https://akkadia.org/drepper/SHA-crypt.txt</a> <a href="https://www.openwall.com/lists/oss-security/2016/01/06">https://www.openwall.com/lists/oss-security/2016/01/06</a>
libgcrypt20	CVE-2024-2236	MEDIUM	1.8.5-5ubuntu1.1		<a href="https://access.redhat.com/security/cve/CVE-2024-2236">https://access.redhat.com/security/cve/CVE-2024-2236</a>
libgssapi-krb5-2	CVE-2024-26462	MEDIUM	1.17-6ubuntu4.7		<a href="https://access.redhat.com/security/cve/CVE-2024-26462">https://access.redhat.com/security/cve/CVE-2024-26462</a>
libgssapi-krb5-2	CVE-2024-26458	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024-3268">https://access.redhat.com/errata/RHSA-2024-3268</a>
libgssapi-krb5-2	CVE-2024-26461	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024-3268">https://access.redhat.com/errata/RHSA-2024-3268</a>
libk5crypto3	CVE-2024-26462	MEDIUM	1.17-6ubuntu4.7		<a href="https://access.redhat.com/security/cve/CVE-2024-26462">https://access.redhat.com/security/cve/CVE-2024-26462</a>
libk5crypto3	CVE-2024-26458	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024-3268">https://access.redhat.com/errata/RHSA-2024-3268</a>
libk5crypto3	CVE-2024-26461	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024-3268">https://access.redhat.com/errata/RHSA-2024-3268</a>
libkrb5-3	CVE-2024-26462	MEDIUM	1.17-6ubuntu4.7		<a href="https://access.redhat.com/security/cve/CVE-2024-26462">https://access.redhat.com/security/cve/CVE-2024-26462</a>

libkrb5-3	CVE-2024-26458	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024:3368">https://access.redhat.com/errata/RHSA-2024:3368</a>
libkrb5-3	CVE-2024-26461	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024:3368">https://access.redhat.com/errata/RHSA-2024:3368</a>
libkrb5support0	CVE-2024-26462	MEDIUM	1.17-6ubuntu4.7		<a href="https://access.redhat.com/security/cve/CVE-2024-26462">https://access.redhat.com/security/cve/CVE-2024-26462</a>
libkrb5support0	CVE-2024-26458	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024:3368">https://access.redhat.com/errata/RHSA-2024:3368</a>
libkrb5support0	CVE-2024-26461	LOW	1.17-6ubuntu4.7		<a href="https://access.redhat.com/errata/RHSA-2024:3368">https://access.redhat.com/errata/RHSA-2024:3368</a>
libncurses6	CVE-2023-45918	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-45918">https://access.redhat.com/security/cve/CVE-2023-45918</a>
libncurses6	CVE-2023-50495	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-50495">https://access.redhat.com/security/cve/CVE-2023-50495</a>
libncursesw6	CVE-2023-45918	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-45918">https://access.redhat.com/security/cve/CVE-2023-45918</a>
libncursesw6	CVE-2023-50495	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-50495">https://access.redhat.com/security/cve/CVE-2023-50495</a>
libpcre2-8-0	CVE-2022-41409	LOW	10.34-7ubuntu0.1		<a href="https://access.redhat.com/security/cve/CVE-2022-41409">https://access.redhat.com/security/cve/CVE-2022-41409</a>
libpcre3	CVE-2017-11164	LOW	2:8.39-12ubuntu0.1		<a href="http://openwall.com/lists/oss-security/2017/07/11/1">http://openwall.com/lists/oss-security/2017/07/11/1</a>
libsystemd0	CVE-2023-26604	LOW	245.4-4ubuntu3.24		<a href="http://packetstormsecurity.com/files/174130/systemd-245.4-4ubuntu3.24-1.tar.xz">http://packetstormsecurity.com/files/174130/systemd-245.4-4ubuntu3.24-1.tar.xz</a>
libsystemd0	CVE-2023-7008	LOW	245.4-4ubuntu3.24		<a href="https://access.redhat.com/errata/RHSA-2024:2466">https://access.redhat.com/errata/RHSA-2024:2466</a>
libtinfo6	CVE-2023-45918	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-45918">https://access.redhat.com/security/cve/CVE-2023-45918</a>
libtinfo6	CVE-2023-50495	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-50495">https://access.redhat.com/security/cve/CVE-2023-50495</a>
libudev1	CVE-2023-26604	LOW	245.4-4ubuntu3.24		<a href="http://packetstormsecurity.com/files/174130/systemd-245.4-4ubuntu3.24-1.tar.xz">http://packetstormsecurity.com/files/174130/systemd-245.4-4ubuntu3.24-1.tar.xz</a>
libudev1	CVE-2023-7008	LOW	245.4-4ubuntu3.24		<a href="https://access.redhat.com/errata/RHSA-2024:2466">https://access.redhat.com/errata/RHSA-2024:2466</a>
login	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.5		<a href="https://access.redhat.com/security/cve/CVE-2013-4235">https://access.redhat.com/security/cve/CVE-2013-4235</a>
login	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.5		<a href="https://access.redhat.com/security/cve/CVE-2023-29383">https://access.redhat.com/security/cve/CVE-2023-29383</a>
ncurses-base	CVE-2023-45918	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-45918">https://access.redhat.com/security/cve/CVE-2023-45918</a>
ncurses-base	CVE-2023-50495	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-50495">https://access.redhat.com/security/cve/CVE-2023-50495</a>
ncurses-bin	CVE-2023-45918	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-45918">https://access.redhat.com/security/cve/CVE-2023-45918</a>
ncurses-bin	CVE-2023-50495	LOW	6.2-0ubuntu2.1		<a href="https://access.redhat.com/security/cve/CVE-2023-50495">https://access.redhat.com/security/cve/CVE-2023-50495</a>
passwd	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.5		<a href="https://access.redhat.com/security/cve/CVE-2013-4235">https://access.redhat.com/security/cve/CVE-2013-4235</a>
passwd	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.5		<a href="https://access.redhat.com/security/cve/CVE-2023-29383">https://access.redhat.com/security/cve/CVE-2023-29383</a>
No Misconfigurations found					
jar					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
com.nimbusds:nimbus-jose-jwt	CVE-2023-52428	HIGH	9.23	9.37.2	<a href="https://access.redhat.com/security/cve/CVE-2023-52428">https://access.redhat.com/security/cve/CVE-2023-52428</a>
net.minidev:json-smart	CVE-2023-1370	HIGH	2.4.8	2.4.9	<a href="https://access.redhat.com/security/cve/CVE-2023-1370">https://access.redhat.com/security/cve/CVE-2023-1370</a>
org.bouncycastle:bc-fips	CVE-2024-29857	MEDIUM	1.0.2.4	1.0.2.5	<a href="https://access.redhat.com/security/cve/CVE-2024-29857">https://access.redhat.com/security/cve/CVE-2024-29857</a>
No Misconfigurations found					

docker.io/velotixai/connector:b3e1d0b-11.05.0828-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
jar					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
commons-io:commons-io	CVE-2024-47554	HIGH	2.8.0	2.14.0	<a href="https://access.redhat.com/security/cve/CVE-2024-47554">https://access.redhat.com/security/cve/CVE-2024-47554</a>
No Misconfigurations found					
python-pkg					
No Vulnerabilities found					
No Misconfigurations found					
dotnet-core					
No Vulnerabilities found					
No Misconfigurations found					
gobinary					
No Vulnerabilities found					
No Misconfigurations found					
dotnet-core					
No Vulnerabilities found					
No Misconfigurations found					

docker.io/velotixai/auth:b3e1d0b-11.05.0828-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
jar					
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Links
commons-io:commons-io	CVE-2024-47554	HIGH	2.8.0	2.14.0	<a href="https://access.redhat.com/security/cve/CVE-2024-47554">https://access.redhat.com/security/cve/CVE-2024-47554</a>
No Misconfigurations found					
gobinary					
No Vulnerabilities found					
No Misconfigurations found					

docker.io/velotixai/proxy:b3e1d0b-11.05.0828-main (wolfi 20230201) - Trivy Report

wolfi					
No Vulnerabilities found					
No Misconfigurations found					
jar					
No Vulnerabilities found					
No Misconfigurations found					

No Vulnerabilities found

No Misconfigurations found