Vulnerability Remediation Plan Template

Table of Contents

1. Asset Identification and Documentation

1.1 Asset Inventory

- **httpd-alpine**
  - Type: Server
  - Owner: Medical Office
  - Function: Web server for EHR system
- **spark**
  - Type: Application
  - Owner: Medical Office
  - Function: Engine for data analytics
- **cassandra**
  - Type: Database
  - Owner: Medical Office
  - Function: Management system for patient data
- **Ubuntu**
  - Type: Operating System
  - Owner: Medical Office
  - Function: Operating system for dental imaging system
- **amazon-linux**
  - Type: Operating System
  - Owner: AWS
  - Function: Operating system for EC2 server

2. Prioritization of Assets

- **Critical Assets:**
  - cassandra due to impact on patient data
  - amazon-linux due to impact on patient records
- **High Priority Assets:**
  - Ubuntu due to impact on patient care
  - spark due to impact on patient care
  - httpd-alpine due to impact on availability and scheduling

3. Prioritization of Vulnerabilities

Using our prioritization of assets in concert with the Common Vulnerability Scoring System (CVSS) we are able to rank the vulnerabilities based on their severity, potential impact, and exploitability. We used Red Hat CVSS scores and NIST CVSS scores to try to maintain comparability. Some vulnerabilities were promoted based on CVSS score and tables are sorted by CVSS score. The above prioritization of assets can be referenced for patching order. An additional mitigation table with immediate actions is provided in remediation plan and a RACI table is used to clarify responsibilities.

3.1 Critical Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
cassandra	org.yaml:snakeyaml	CVE-2022-1471	HIGH	1.26	2.0	unauthenticated remote code execution	9.8
ubuntu	libudev1	CVE-2022-2526	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.56	use-after-free	9.8
ubuntu	libsystemd0	CVE-2022-2526	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.56	use-after-free	9.8
spark	org.apache.derby:derby	CVE-2022-46337	CRITICAL	10.14.2.0	10.17.1.0	LDAP injection vulnerability, bypass authentication	9.8
ubuntu	dpkg	CVE-2022-1664	MEDIUM	1.19.0.5ubuntu2.3	1.19.0.5ubuntu2.4	directory traversal	9.8
spark	org.apache.zookeeper:zookeeper	CVE-2023-44981	CRITICAL	3.6.3	3.7.2, 3.8.3, 3.9.1	Authorization Bypass	9.1
ubuntu	gzip	CVE-2022-1271	MEDIUM	1.6-5ubuntu1	1.6-5ubuntu1.2	arbitrary file write	8.8
cassandra	python3.8	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass of TLS handshake	8.6
cassandra	python3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass of the TLS handshake	8.6
cassandra	libpython3.8-stdlib	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass of TLS handshake	8.6
cassandra	libpython3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass of the TLS handshake	8.6
spark	org.apache.ivy:ivy	CVE-2022-46751	HIGH	2.5.1	2.5.2	XML injection	8.2
httpd-alpine	libcurl	CVE-2023-38545	CRITICAL	7.88.1-r1	8.4.0-r0	buffer overflow flaw possible to execute arbitrary code	8.1
spark	org.codehaus.jackson:jackson-mapper-asl	CVE-2019-10202	CRITICAL	1.9.13		A series of deserialization vulnerabilities	8.1
amazon-linux	libcurl	CVE-2023-38545	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	execute arbitrary code	8.1
amazon-linux	curl	CVE-2023-38545	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	Buffer overflow	8.1

3.2 High-Priority Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
amazon-linux	vim-minimal	CVE-2023-4781	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	buffer overflow	7.8
amazon-linux	vim-minimal	CVE-2023-4734	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	integer overflow	7.8
amazon-linux	vim-minimal	CVE-2023-4733	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	use-after-free	7.8
amazon-linux	vim-minimal	CVE-2023-4751	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	buffer overflow	7.8
amazon-linux	vim-minimal	CVE-2023-4750	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	use-after-free	7.8
amazon-linux	vim-minimal	CVE-2023-4738	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	buffer overflow	7.8
amazon-linux	vim-data	CVE-2023-4781	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	Buffer overflow	7.8
amazon-linux	vim-data	CVE-2023-4734	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	integer overflow	7.8
amazon-linux	vim-data	CVE-2023-4733	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	use-after-free	7.8
amazon-linux	python-libs	CVE-2022-48565	HIGH	2.7.18-1.amzn2.0.6	2.7.18-1.amzn2.0.7	obtain sensitive information and Denial of Service	7.8
amazon-linux	python	CVE-2022-48565	HIGH	2.7.18-1.amzn2.0.6	2.7.18-1.amzn2.0.7	Denial of Service	7.8
amazon-linux	vim-data	CVE-2023-4751	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	Buffer overflow	7.8
amazon-linux	vim-data	CVE-2023-4750	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	use-after-free	7.8
amazon-linux	vim-data	CVE-2023-4738	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	Buffer overflow	7.8
spark	linux-libc-dev	CVE-2022-47519	LOW	5.4.0-166.183		crash and escalation of privileges important	7.8
spark	linux-libc-dev	CVE-2022-47518	LOW	5.4.0-166.183		crash and escalation of privileges important	7.8
spark	com.squareup.okio:okio	CVE-2023-3635	MEDIUM	1.15.0	3.4.0, 1.17.6	denial of service important	7.5
httpd-alpine	nghttp2-libs	CVE-2023-44487	HIGH	1.51.0-r0	1.51.0-r2	Denial of Service	7.5
httpd-alpine	nghttp2-libs	CVE-2023-35945	HIGH	1.51.0-r0	1.51.0-r1	Denial of Service	7.5
httpd-alpine	libssl3	CVE-2023-5363	HIGH	3.0.8-r3	3.0.12-r0	loss of confidentiality	7.5
httpd-alpine	libcurl	CVE-2023-38039	HIGH	7.88.1-r1	8.3.0	out of memory crash	7.5
httpd-alpine	libcurl	CVE-2023-28319	HIGH	7.88.1-r1	8.1.0-r0	use-after-free	7.5
httpd-alpine	libcrypto3	CVE-2023-5363	HIGH	3.0.8-r3	3.0.12-r0	loss of confidentiality	7.5
spark	com.fasterxml.jackson.core:jackson-databind	CVE-2022-42003	HIGH	2.12.7	2.12.7.1, 2.13.4.2	resource exhaustion	7.5
spark	com.fasterxml.jackson.core:jackson-databind	CVE-2022-42004	HIGH	2.12.7	2.12.7.1, 2.13.4	resource exhaustion	7.5
spark	com.google.code.gson:gson	CVE-2022-25647	HIGH	2.2.4	2.8.9	availability attacks	7.5
spark	com.google.protobuf:protobuf-java	CVE-2021-22570	HIGH	3.3.0	3.15.0	execute unauthorized code or commands,	7.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
						read memory, modify memory	
spark	com.google.protobuf:protobuf-java	CVE-2022-3509	HIGH	3.3.0	3.16.3, 3.19.6, 3.20.3, 3.21.7	Denial of Service	7.5
spark	com.google.protobuf:protobuf-java	CVE-2022-3510	HIGH	3.3.0	3.16.3, 3.19.6, 3.20.3, 3.21.7	Denial of Service	7.5
spark	com.google.protobuf:protobuf-java	CVE-2021-22570	HIGH	3.7.1	3.15.0	execute unauthorized code or commands, read memory, modify memory	7.5
spark	com.google.protobuf:protobuf-java	CVE-2022-3509	HIGH	3.7.1	3.16.3, 3.19.6, 3.20.3, 3.21.7	Denial of Service	7.5
spark	com.google.protobuf:protobuf-java	CVE-2022-3510	HIGH	3.7.1	3.16.3, 3.19.6, 3.20.3, 3.21.7	Denial of Service	7.5
spark	io.netty:netty-codec-http2	GHSA-xpw8-rcwv-8f8p	HIGH	4.1.96.Final	4.1.100.Final	Denial of Service	7.5
spark	net.minidev:json-smart	CVE-2021-31684	HIGH	1.3.2	1.3.3, 2.4.4	Denial of Service	7.5
spark	net.minidev:json-smart	CVE-2023-1370	HIGH	1.3.2	2.4.9	stack overflow crash software	7.5
spark	org.apache.avro:avro	CVE-2023-39410	HIGH	1.11.2	1.11.3	out of memory error and denial of service	7.5
spark	org.apache.avro:avro	CVE-2023-39410	HIGH	1.7.7	1.11.3	out of memory error and denial of service	7.5
spark	linux-libc-dev	CVE-2023-45871	MEDIUM	5.4.0-166.183	5.4.0-167.184	system integrity	7.5
spark	org.xerial.snappy:snappy-java	CVE-2023-43642	HIGH	1.1.10.3	1.1.10.4	Denial of Service	7.5
spark	org.apache.thrift:libthrift	CVE-2020-13949	HIGH	0.12.0	0.14.0	Denial of service	7.5
spark	org.apache.mesos:mesos	CVE-2018-1330	HIGH	1.4.3	1.6.0	Denial of Service	7.5
amazon-linux	libssh2	CVE-2020-22218	HIGH	1.4.3-12.amzn2.2.4	1.4.3-12.amzn2.2.6	application crash	7.5
amazon-linux	libnghttp2	CVE-2023-44487	HIGH	1.41.0-1.amzn2.0.1	1.41.0-1.amzn2.0.4	Denial of Service	7.5
amazon-linux	curl	CVE-2023-38039	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.1	Run out of memory possible crash	7.5
cassandra	libc6	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
cassandra	libc-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
cassandra	locales	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
cassandra	github.com/opencontainers/runc	CVE-2023-27561	HIGH	v1.1.0	1.1.5	Access Control Privilege Escalation	7.5
cassandra	libnghttp2-14	CVE-2023-44487	MEDIUM	1.40.0-1ubuntu0.1	1.40.0-1ubuntu0.2	Denial of Service active exploit	7.5
cassandra	org.yaml:snakeyaml	CVE-2022-25857	HIGH	1.26	1.31	Denial of Service	7.5
cassandra	org.xerial.snappy:snappy-java	CVE-2023-43642	HIGH	1.1.10.1	1.1.10.4	Denial of Service	7.5
cassandra	com.fasterxml.jackson.core:jackson-databind	CVE-2022-42004	HIGH	2.13.2.2	2.12.7.1, 2.13.4	resource exhaustion	7.5
cassandra	com.fasterxml.jackson.core:jackson-databind	CVE-2022-42003	HIGH	2.13.2.2	2.12.7.1, 2.13.4.2	resource exhaustion	7.5
cassandra	ch.qos.logback:logback-core	CVE-2023-6378	HIGH	1.2.9	1.3.12, 1.4.12	Denial of Service	7.5
cassandra	ch.qos.logback:logback-classic	CVE-2023-	HIGH	1.2.9	1.3.12, 1.4.12	Denial of Service	7.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
		6378					
amazon-linux	libcurl	CVE-2023-38039	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.1	run out of memory	7.5
spark	linux-libc-dev	CVE-2019-14899	LOW	5.4.0-166.183		hijack active VPN connection important	7.4
amazon-linux	vim-minimal	CVE-2023-4735	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	out of bounds wirte	7.3
amazon-linux	vim-data	CVE-2023-4735	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	out-of-bounds write	7.3
cassandra	perl-base	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5	regular expression buffer overflow	7.0
httpd-alpine	perl	CVE-2023-47038	HIGH	5.36.0-r0	5.36.2-r0	regular expression buffer overflow	7.0
spark	linux-libc-dev	CVE-2023-4244	HIGH	5.4.0-166.183		use-after-free kernel information leak	7.0
amazon-linux	vim-minimal	CVE-2023-4752	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	crash software and possible code execution	7.0
amazon-linux	vim-data	CVE-2023-4752	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	crash software and possible code execution	7.0
spark	org.codehaus.jackson:jackson-mapper-asl	CVE-2019-10172	HIGH	1.9.13		data integrity	5.9
spark	org.apache.thrift:libthrift	CVE-2019-0205	HIGH	0.12.0	0.13.0	endless loop	5.9
amazon-linux	libxml2	CVE-2023-45322	HIGH	2.9.1-6.amzn2.5.8	2.9.1-6.amzn2.5.13	use-after-free memory attack	5.9
spark	linux-libc-dev	CVE-2023-20569	HIGH	5.4.0-166.183		potential information disclosure	5.6
Ubuntu	libudev1	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	OS Crash	5.5
Ubuntu	libsystemd0	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	OS Crash	5.5
spark	com.google.protobuf:protobuf-java	CVE-2021-22569	HIGH	3.3.0	3.16.1, 3.18.2, 3.19.2	Denial of Service	5.5
spark	com.google.protobuf:protobuf-java	CVE-2021-22569	HIGH	3.7.1	3.16.1, 3.18.2, 3.19.2	Denial of Service	5.5
amazon-linux	vim-minimal	CVE-2021-3236	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	pointer dereference	5.5
amazon-linux	vim-data	CVE-2021-3236	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	pointer dereference causes crash	5.5

3.3 Medium-Priority Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	libctf0	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
spark	libctf-nobfd0	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
spark	libbinutils	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
spark	binutils-x86-64-linux-gnu	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
spark	binutils-common	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
spark	binutils	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6		denial of service and read/write memory	8.8
ubuntu	liblzma5	CVE-2022-1271	MEDIUM	5.2.2-1.3	5.2.2-1.3ubuntu0.1	arbitrary file write	8.8
spark	python3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass TSL handshake	8.6
spark	python3.8-dev	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass TSL handshake	8.6
spark	python3.8	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9	bypass TSL handshake	8.6
ubuntu	liblz4-1	CVE-2021-3520	MEDIUM	0.0~r131-2ubuntu3	0.0~r131-2ubuntu3.1	out-of-bounds write and/or crash	8.6
ubuntu	zlib2g	CVE-2018-25032	MEDIUM	1:1.2.11.dfsg-0ubuntu2	1:1.2.11.dfsg-0ubuntu2.1	corruption and crash	8.2
ubuntu	libnettle6	CVE-2021-20305	MEDIUM	3.4-1	3.4-1ubuntu0.1	force invalid signature	8.1
ubuntu	libhogweed4	CVE-2021-20305	MEDIUM	3.4-1	3.4-1ubuntu0.1	force invalid signature	8.1
spark	linux-libc-dev	CVE-2023-26242	MEDIUM	5.4.0-166.183		integer overflow	7.8
spark	linux-libc-dev	CVE-2022-1247	MEDIUM	5.4.0-166.183		kernel race condition	7.8
spark	linux-libc-dev	CVE-2020-12362	MEDIUM	5.4.0-166.183		privilege escalation	7.8
spark	libctf0	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	libctf0	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	libctf0	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	libctf-nobfd0	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	libctf-nobfd0	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	libctf-nobfd0	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	libbinutils	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	libbinutils	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	libbinutils	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	binutils-x86-64-linux-gnu	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	binutils-x86-64-linux-gnu	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	binutils-x86-64-linux-gnu	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	binutils-common	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	binutils-common	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	binutils-common	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	binutils	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6		denial of service	7.8
spark	binutils	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
spark	binutils	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.8
ubuntu	perl-base	CVE-2020-16156	MEDIUM	5.26.1-6ubuntu0.3	5.26.1-6ubuntu0.6	bypass signature verification	7.8
ubuntu	ncurses-bin	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	memory corruption	7.8
ubuntu	ncurses-base	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	memory corruption	7.8
ubuntu	libudev1	CVE-2020-1712	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.38	use-after-free	7.8
ubuntu	libtinfo5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	memory corruption	7.8
ubuntu	libsystemd0	CVE-2020-1712	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.38	use-after-free	7.8
ubuntu	libncursesw5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	memory corruption	7.8
ubuntu	libncurses5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	memory corruption	7.8
ubuntu	libc6	CVE-2018-11236	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	buffer overflow and code execution	7.8
ubuntu	libc-bin	CVE-2018-11236	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	buffer overflow and code execution	7.8
cassandra	github.com/opencontainers/runc	CVE-2023-28642	MEDIUM	v1.1.0	1.1.5	bypass security restrictions	7.8
spark	com.google.protobuf:protobuf-java	CVE-2022-3171	MEDIUM	3.7.1	3.21.7, 3.20.3, 3.19.6, 3.16.3	denial of service	7.5
spark	com.google.protobuf:protobuf-java	CVE-2022-3171	MEDIUM	3.3.0	3.21.7, 3.20.3, 3.19.6, 3.16.3	denial of service	7.5
spark	com.fasterxml.woodstox:woodstox-core	CVE-2022-40152	MEDIUM	5.3.0	6.4.0, 5.4.0	denial of service	7.5
spark	locales	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
spark	linux-libc-dev	CVE-2023-39198	MEDIUM	5.4.0-166.183		denial of service	7.5
spark	linux-libc-dev	CVE-2022-25836	MEDIUM	5.4.0-166.183		bluetooth passkey leak	7.5
spark	linux-libc-dev	CVE-2022-0400	MEDIUM	5.4.0-166.183		denial of service	7.5
spark	libnghttp2-14	CVE-2023-44487	MEDIUM	1.40.0-1ubuntu0.1	1.40.0-1ubuntu0.2		denial of service

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	libctf0	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
spark	libctf-nobfd0	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
spark	libc6-dev	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
spark	libc6	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
spark	libc-dev-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
spark	libc-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12		memory leak	7.5
spark	libbinutils	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
spark	binutils-x86-64-linux-gnu	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
spark	binutils-common	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
spark	binutils	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6		buffer overflow	7.5
ubuntu	libss2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.3	code execution	7.5
ubuntu	libp11-kit0	CVE-2020-29363	MEDIUM	0.23.9-2	0.23.9-2ubuntu0.1	buffer overflow	7.5
ubuntu	libp11-kit0	CVE-2020-29361	MEDIUM	0.23.9-2	0.23.9-2ubuntu0.1	integer overflow	7.5
ubuntu	libnettle6	CVE-2021-3580	MEDIUM	3.4-1	3.4.1-0ubuntu0.18.04.1	denial of service	7.5
ubuntu	libhogweed4	CVE-2021-3580	MEDIUM	3.4-1	3.4.1-0ubuntu0.18.04.1	denial of service	7.5
ubuntu	libgnutls30	CVE-2022-2509	MEDIUM	3.5.18-1ubuntu1.2	3.5.18-1ubuntu1.6	double-free error	7.5
ubuntu	libext2fs2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.3	code execution	7.5
ubuntu	libcom-err2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.3	code execution	7.5
ubuntu	e2fsprogs	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.3	code execution	7.5
amazon-linux	curl	CVE-2023-28319	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	leak sensitive information	7.5
ubuntu	perl-base	CVE-2023-31484	MEDIUM	5.26.1-6ubuntu0.3	5.26.1-6ubuntu0.7	man-in-the-middle	7.4
ubuntu	libc6	CVE-2021-3999	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.5	code execution Privilege escalation	7.4
ubuntu	libc-bin	CVE-2021-3999	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.5	code execution Privilege escalation	7.4
spark	perl-modules-5.30	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5	regular expression buffer overflow	7.0
spark	perl-base	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5	regular expression buffer overflow	7.0
spark	perl	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5	regular expression buffer overflow	7.0
spark	linux-libc-dev	CVE-2023-0030	MEDIUM	5.4.0-166.183		escalation of privileges	7.0

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	linux-libc-dev	CVE-2022-39189	MEDIUM	5.4.0-166.183		comprimise guest kernel	7.0
spark	linux-libc-dev	CVE-2022-1280	MEDIUM	5.4.0-166.183		denial of service kernel leak	7.0
spark	linux-libc-dev	CVE-2021-3864	MEDIUM	5.4.0-166.183		privilege escalation	7.0
spark	libperl5.30	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5	regular expression buffer overflow	7.0
ubuntu	zlib1g	CVE-2022-37434	MEDIUM	1:1.2.11.dfsg-0ubuntu2	1:1.2.11.dfsg-0ubuntu2.2	buffer over-read	7.0
ubuntu	libc6	CVE-2020-1751	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	out-of-bounds write	7.0
ubuntu	libc-bin	CVE-2020-1751	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	denial of service	7.0
spark	linux-libc-dev	CVE-2023-39192	MEDIUM	5.4.0-166.183		crash and information disclosure	6.7
spark	linux-libc-dev	CVE-2023-2007	MEDIUM	5.4.0-166.183		escalation of privileges	6.7
httpd-alpine	libssl3	CVE-2023-2650	MEDIUM	3.0.8-r3	3.0.9-r0	denial of service	6.5
httpd-alpine	libcrypto3	CVE-2023-2650	MEDIUM	3.0.8-r3	3.0.9-r0	denial of service	6.5
spark	wget	CVE-2021-31879	MEDIUM	1.20.3-1ubuntu2		password leak	6.5
spark	linux-libc-dev	CVE-2022-3344	MEDIUM	5.4.0-166.183		kernel panic	6.5
spark	linux-libc-dev	CVE-2022-2961	MEDIUM	5.4.0-166.183		crash or escalation of privileges	6.5
spark	linux-libc-dev	CVE-2020-26144	MEDIUM	5.4.0-166.183		authentication bypass	6.5
spark	libnss3	CVE-2023-5388	MEDIUM	2:3.49.1-1ubuntu1.9		cryptography leak	6.5
spark	libnss3	CVE-2023-4421	MEDIUM	2:3.49.1-1ubuntu1.9		information leak	6.5
spark	libkrb5support0	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libkrb5-3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libkdb5-9	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libkadm5srv-mit11	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libkadm5clnt-mit11	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libk5crypto3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libgssrpc4	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	libgssapi-krb5-2	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
spark	krb5-user	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
amazon-linux	libxml2	CVE-2023-39615	MEDIUM	2.9.1-6.amzn2.5.8	2.9.1-6.amzn2.5.11	denial of service	6.5
amazon-linux	krb5-libs	CVE-2023-36054	MEDIUM	1.15.1-55.amzn2.2.5	1.15.1-55.amzn2.2.6	denial of service	6.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
amazon-linux	expat	CVE-2022-25313	MEDIUM	2.1.0-15.amzn2.0.2	2.1.0-15.amzn2.0.3	denial of service	6.5
amazon-linux	expat	CVE-2022-23990	MEDIUM	2.1.0-15.amzn2.0.2	2.1.0-15.amzn2.0.3	denial of service	6.5
cassandra	org.yaml:snakeyaml	CVE-2022-41854	MEDIUM	1.26	1.32	denial of service	6.5
cassandra	org.yaml:snakeyaml	CVE-2022-38752	MEDIUM	1.26	1.32	application crash	6.5
cassandra	org.yaml:snakeyaml	CVE-2022-38751	MEDIUM	1.26	1.31	application crash	6.5
cassandra	org.yaml:snakeyaml	CVE-2022-38749	MEDIUM	1.26	1.31	denial of service	6.5
cassandra	wget	CVE-2021-31879	MEDIUM	1.20.3-1ubuntu2		password leak	6.5
cassandra	libkrb5support0	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
cassandra	libkrb5-3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
cassandra	libk5crypto3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	denial of service	6.5
cassandra	libgssapi-krb5-2	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu4.4	Denial of Service	6.5
spark	linux-libc-dev	CVE-2023-45863	MEDIUM	5.4.0-166		escalation of privileges	6.4
spark	linux-libc-dev	CVE-2020-27835	MEDIUM	5.4.0-166.183		crash system	6.4
ubuntu	libgcrypt20	CVE-2019-13627	MEDIUM	1.8.1-4ubuntu1.1	1.8.1-4ubuntu1.2	timing attack	6.3
spark	python-pip-whl	CVE-2018-25091	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	expose credentials	6.1
spark	linux-libc-dev	CVE-2023-39193	MEDIUM	5.4.0-166.183		crash and information disclosure	6.1
httpd-alpine	libxml2	CVE-2023-29469	MEDIUM	2.10.3-r1	2.10.4-r0	logic and memory errors	5.9
httpd-alpine	libxml2	CVE-2023-28484	MEDIUM	2.10.3-r1	2.10.4-r0	pointer dereference	5.9
httpd-alpine	libcurl	CVE-2023-28321	MEDIUM	7.88.1-r1	8.1.0-r0	improper certificate validation	5.9
spark	com.google.guava:guava	CVE-2018-10237	MEDIUM	14.0.1	24.1.1-android	denial of service	5.9
spark	com.google.guava:guava	CVE-2018-10237	MEDIUM	14.0.1	24.1.1-android	denial of service	5.9
spark	python3-pip	CVE-2023-45803	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	information leak	5.9
spark	python3-pip	CVE-2023-43804	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	information leak	5.9
spark	python-pip-whl	CVE-2023-45803	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	information leak	5.9
spark	python-pip-whl	CVE-2023-43804	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	information leak	5.9
spark	libgnutls30	CVE-2023-5981	MEDIUM	3.6.13-2ubuntu1.8	3.6.13-2ubuntu1.9	side channel	5.9
ubuntu	libgcrypt20	CVE-2021-40528	MEDIUM	1.8.1-4ubuntu1.1	1.8.1-4ubuntu1.3	plain text recovery	5.9
ubuntu	gpgv	CVE-2022-34903	MEDIUM	2.2.4-1ubuntu1.2	2.2.4-1ubuntu1.6	bypass access control	5.9

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
amazon-linux	libcurl	CVE-2023-28321	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	improper certificate validation	5.9
amazon-linux	libcurl	CVE-2023-28319	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	sensitive information leak	5.9
amazon-linux	curl	CVE-2023-28321	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	improper certificate validation	5.9
cassandra	libgnutls30	CVE-2023-5981	MEDIUM	3.6.13-2ubuntu1.8	3.6.13-2ubuntu1.9	response time discrepancy	5.9
ubuntu	libss2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.4	out-of-bounds read/write	5.8
ubuntu	libext2fs2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.4	out-of-bounds read/write	5.8
ubuntu	libcom-err2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.4	out-of-bounds read/write	5.8
ubuntu	e2fsprogs	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2	1.44.1-1ubuntu1.4	code execution	5.8
ubuntu	libapt-pkg5.0	CVE-2020-27350	MEDIUM	1.6.12	1.6.12ubuntu0.2	integer overflow	5.7
ubuntu	apt	CVE-2020-27350	MEDIUM	1.6.12	1.6.12ubuntu0.2	integer overflow	5.7
ubuntu	libc6	CVE-2018-11237	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	denial of service	5.6
ubuntu	libc-bin	CVE-2018-11237	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	buffer overflow and code execution	5.6
cassandra	github.com/opencontainers/runc	CVE-2022-29162	MEDIUM	v1.1.0	1.1.2	incorrect default permissions	5.6
spark	org.apache.commons:commons-compress	CVE-2023-42503	MEDIUM	1.23.0	1.24.0	uncontrolled resource consumption	5.5
spark	xz-utils	CVE-2020-22916	MEDIUM	5.2.4-1ubuntu1.1		denial of service	5.5
spark	linux-libc-dev	CVE-2023-31082	MEDIUM	5.4.0-166.183		local system crash	5.5
spark	linux-libc-dev	CVE-2023-28327	MEDIUM	5.4.0-166.183		local denial of service	5.5
spark	linux-libc-dev	CVE-2023-23004	MEDIUM	5.4.0-166.183		local user crash	5.5
spark	linux-libc-dev	CVE-2022-4543	MEDIUM	5.4.0-166.183		EntryBleed	5.5
spark	linux-libc-dev	CVE-2022-40133	MEDIUM	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2022-38457	MEDIUM	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2022-38096	MEDIUM	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2022-36402	MEDIUM	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2022-0480	MEDIUM	5.4.0-166.183		memory exhaustion	5.5
spark	linux-libc-dev	CVE-2020-36310	MEDIUM	5.4.0-166.183		infinite loop	5.5
spark	linux-libc-dev	CVE-2020-24504	MEDIUM	5.4.0-166.183		local access denial of service	5.5
spark	linux-libc-dev	CVE-2016-8660	MEDIUM	5.4.0-166.183		denial of service	5.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	liblzma5	CVE-2020-22916	MEDIUM	5.2.4-1ubuntu1.1		denial of service	5.5
spark	libctf0	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	libctf0	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	libctf0	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf0	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf0	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf0	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf0	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
spark	libctf-nobfd0	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf-nobfd0	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	libctf-nobfd0	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf-nobfd0	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf-nobfd0	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf-nobfd0	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libctf-nobfd0	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
spark	libbinutils	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libbinutils	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	libbinutils	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libbinutils	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libbinutils	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libbinutils	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	libbinutils	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
spark	gcc	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2		side channel	5.5
spark	g++	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2		side channel	5.5
spark	cpp	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2		side channel	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	binutils-x86-64-linux-gnu	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
spark	binutils-common	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-common	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	binutils-common	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-common	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-common	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-common	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils-common	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
spark	binutils	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6		excessive memory usage	5.5
spark	binutils	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6		memory leak	5.5
spark	binutils	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6		denial of service	5.5
ubuntu	tar	CVE-2022-48303	MEDIUM	1.29b-2ubuntu0.1	1.29b-2ubuntu0.4	expose sensitive information	5.5
ubuntu	libzstd1	CVE-2021-24032	MEDIUM	1.3.3+dfsg-2ubuntu1.1	1.3.3+dfsg-2ubuntu1.2	temporary permission gain	5.5
ubuntu	libzstd1	CVE-2021-24031	MEDIUM	1.3.3+dfsg-2ubuntu1.1	1.3.3+dfsg-2ubuntu1.2	temporary permission gain	5.5
ubuntu	libudev1	CVE-2022-3821	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.57	denial of service	5.5
ubuntu	libsystemd0	CVE-2022-3821	MEDIUM	237-3ubuntu10.33	237-3ubuntu10.57	denial of service	5.5
ubuntu	libapt-pkg5.0	CVE-2020-3810	MEDIUM	1.6.12	1.6.12ubuntu0.1	denial of service	5.5
ubuntu	apt	CVE-2020-3810	MEDIUM	1.6.12	1.6.12ubuntu0.1	denial of service	5.5
amazon-linux	vim-minimal	CVE-2023-5441	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.3	application crash	5.5
amazon-linux	vim-data	CVE-2023-5441	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.3	application crash	5.5
amazon-linux	elfutils-libelf	CVE-2020-21047	MEDIUM	0.176-2.amzn2.0.1	0.176-2.amzn2.0.2	denial of service	5.5
cassandra	org.yaml:snakeyaml	CVE-2022-38750	MEDIUM	1.26	1.31	application crash	5.5
cassandra	liblzma5	CVE-2020-22916	MEDIUM	5.2.4-1ubuntu1.1		denial of service	5.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
httpd-alpine	libssl3	CVE-2023-5678	MEDIUM	3.0.8-r3	3.0.12-r1	denial of service	5.3
httpd-alpine	libssl3	CVE-2023-3817	MEDIUM	3.0.8-r3	3.0.10-r0	denial of service	5.3
httpd-alpine	libssl3	CVE-2023-3446	MEDIUM	3.0.8-r3	3.0.9-r3	denial of service	5.3
httpd-alpine	libssl3	CVE-2023-2975	MEDIUM	3.0.8-r3	3.0.9-r2	empty data not authenticated	5.3
httpd-alpine	libcrypto3	CVE-2023-5678	MEDIUM	3.0.8-r3	3.0.12-r1	denial of service	5.3
httpd-alpine	libcrypto3	CVE-2023-3817	MEDIUM	3.0.8-r3	3.0.10-r0	denial of service	5.3
httpd-alpine	libcrypto3	CVE-2023-3446	MEDIUM	3.0.8-r3	3.0.9-r3	denial of service	5.3
httpd-alpine	libcrypto3	CVE-2023-2975	MEDIUM	3.0.8-r3	3.0.9-r2	empty data not authenticated	5.3
spark	org.eclipse.jetty:jetty-http	CVE-2023-40167	MEDIUM	9.4.43.v20210629	9.4.52, 10.0.16, 11.0.16, 12.0.1	improper validation	5.3
spark	python3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	python3.8-dev	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	python3.8	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	linux-libc-dev	CVE-2022-3523	MEDIUM	5.4.0-166.183		use after free	5.3
spark	linux-libc-dev	CVE-2015-8553	MEDIUM	5.4.0-166.183		sensitive information leak	5.3
spark	libpython3.8-stdlib	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	libpython3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	libpython3.8-dev	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
spark	libpython3.8	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
ubuntu	libp11-kit0	CVE-2020-29362	MEDIUM	0.23.9-2	0.23.9-2ubuntu0.1	buffer over-read	5.3
ubuntu	libc6	CVE-2018-19591	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	uncontrolled resource usage	5.3
ubuntu	libc-bin	CVE-2018-19591	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	uncontrolled resource usage	5.3
amazon-linux	zlib	CVE-2023-45853	MEDIUM	1.2.7-19.amzn2.0.2	1.2.7-19.amzn2.0.3	out-of-bounds write	5.3
amazon-linux	vim-minimal	CVE-2023-5344	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.2	denial of service	5.3
amazon-linux	vim-data	CVE-2023-5344	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.2	denial of service	5.3
amazon-linux	openssl-libs	CVE-2023-3817	MEDIUM	1:1.0.2k-24.amzn2.0.7	1:1.0.2k-24.amzn2.0.9	denial of service	5.3
amazon-linux	openssl-libs	CVE-2023-3446	MEDIUM	1:1.0.2k-24.amzn2.0.7	1:1.0.2k-24.amzn2.0.9	denial of service	5.3
cassandra	python3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
cassandra	python3.8	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
cassandra	libpython3.8-stdlib	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
cassandra	libpython3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8		incorrectly parse email	5.3
httpd-alpine	libssl3	CVE-2023-1255	MEDIUM	3.0.8-r3	3.0.8-r4	crash	5.1
httpd-alpine	libcrypto3	CVE-2023-1255	MEDIUM	3.0.8-r3	3.0.8-r4	crash	5.1
spark	linux-libc-dev	CVE-2023-23000	MEDIUM	5.4.0-166.183		local user crash	5.1
spark	linux-libc-dev	CVE-2021-4148	MEDIUM	5.4.0-166.183		denial of service	5.1
sprak	linux-libc-dev	CVE-2023-34324	MEDIUM	5.4.0-166.183		kernel deadlock	4.9
spark	linux-libc-dev	CVE-2018-17977	MEDIUM	5.4.0-166.183		use all memory	4.9
spark	linux-libc-dev	CVE-2023-4732	MEDIUM	5.4.0-166.183		local denial of service	4.7
spark	linux-libc-dev	CVE-2023-3006	MEDIUM	5.4.0-166.183		cache speculation information disclosure	4.7
spark	linux-libc-dev	CVE-2023-1582	MEDIUM	5.4.0-166.183		local denial of service	4.7
spark	linux-libc-dev	CVE-2023-37453	MEDIUM	5.4.0-166.183		out of bounds crash	4.6
spark	com.google.guava:guava	CVE-2023-2976	MEDIUM	30.1.1-jre	32.0.0-android	information exposure	4.4
spark	com.google.guava:guava	CVE-2023-2976	MEDIUM	30.1.1-jre	32.0.0-android	information exposure	4.4
spark	com.google.guava:guava	CVE-2023-2976	MEDIUM	14.0.1	32.0.0-android	information exposure	4.4
spark	com.google.guava:guava	CVE-2023-2976	MEDIUM	14.0.1	32.0.0-android	information exposure	4.4
spark	linux-libc-dev	CVE-2022-29900	MEDIUM	5.4.0-166.183		kernel leak	4.4
cassandra	com.google.guava:guava	CVE-2023-2976	MEDIUM	27.0-jre	32.0.0-android	information exposure	4.4
spark	linux-libc-dev	CVE-2013-7445	MEDIUM	5.4.0-166.183		denial of service	4.3
spark	python3-pip	CVE-2018-25091	MEDIUM	20.0.2-5ubuntu1.9	20.0.2-5ubuntu1.10	HTTP information leak	4.2
amazon-linux	vim-minimal	CVE-2023-46246	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.2081-1.amzn2.0.1	integer overflow	4.0
amazon-linux	vim-data	CVE-2023-46246	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.2081-1.amzn2.0.1	integer overflow	4.0
httpd-alpine	libcurl	CVE-2023-28320	MEDIUM	7.88.1-r1	8.1.0-r0	denial of service	3.7
amazon-linux	libcurl	CVE-2023-28322	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	information leak	3.7
amazon-linux	curl	CVE-2023-28322	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	information leak	3.7
spark	commons-net:commons-net	CVE-2021-37533	MEDIUM	3.6	3.9.0	information leakage	6.5
spark	tar	CVE-2023-39804	MEDIUM	1.30+dfsg-7ubuntu0.20.04.3		denial of service	3.3
amazon-linux	vim-minimal	CVE-2023-5535	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.3	system compromise user run untrusted file	3.3

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
amazon-linux	vim-data	CVE-2023-5535	MEDIUM	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.3	system compromise user run untrusted file	3.3
amazon-linux	libsepol	CVE-2021-36087	MEDIUM	2.5-8.1.amzn2.0.2	2.5-10.amzn2.0.1	buffer over-read	3.3
amazon-linux	libsepol	CVE-2021-36086	MEDIUM	2.5-8.1.amzn2.0.2	2.5-10.amzn2.0.1	use-after-free	3.3
amazon-linux	libsepol	CVE-2021-36085	MEDIUM	2.5-8.1.amzn2.0.2	2.5-10.amzn2.0.1	use-after-free	3.3
amazon-linux	libsepol	CVE-2021-36084	MEDIUM	2.5-8.1.amzn2.0.2	2.5-10.amzn2.0.1	use-after-free	3.3
amazon-linux	libcurl	CVE-2020-19909	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	integer overflow	3.3
amazon-linux	curl	CVE-2020-19909	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	integer overflow	3.3
cassandra	tar	CVE-2023-39804	MEDIUM	1.30+dfsg-7ubuntu0.20.04.3		denial of service	3.3
spark	libpython3.8-stdlib	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9		
spark	libpython3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9		
spark	libpython3.8-dev	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9		
spark	libpython3.8	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20.04.9		
amazon-linux	libstdc++	CVE-2023-4039	MEDIUM	7.3.1-15.amzn2	7.3.1-17.amzn2	change program flow	0.0-4.8
amazon-linux	libgcc	CVE-2023-4039	MEDIUM	7.3.1-15.amzn2	7.3.1-17.amzn2	change program flow *disputed	0.0-4.8

3.4 Low-Priority Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
ubuntu	libc6	CVE-2021-35942	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	integer overflow untrusted regular expression	9.1
ubuntu	libc-bin	CVE-2021-35942	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	integer overflow untrusted regular expression	9.1
ubuntu	perl-base	CVE-2020-10878	LOW	5.26.1-6ubuntu0.3	5.26.1-6ubuntu0.5	regular expression instruction injection	8.6
spark	linux-libc-dev	CVE-2021-32078	LOW	5.4.0-166.183		out-of-bounds read	8.4
ubuntu	perl-base	CVE-2020-10543	LOW	5.26.1-6ubuntu0.3	5.26.1-6ubuntu0.5	nested regular expression integer overflow	8.2
ubuntu	libc-bin	CVE-2020-6096	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	out-of-bounds write	8.1
ubuntu	libc6	CVE-2020-6096	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	out-of-bounds write	8.1
ubuntu	bash	CVE-2019-18276	LOW	4.4.18-2ubuntu1.2	4.4.18-2ubuntu1.3	low impact privilege escalation	7.8
spark	linux-libc-dev	CVE-2021-39801	LOW	5.4.0-166.183		privilege escalation	7.8
spark	linux-libc-dev	CVE-2021-26934	LOW	5.4.0-166.183		be-alloc not supported	7.8
spark	linux-libc-dev	CVE-2019-19378	LOW	5.4.0-166.183		low impact BTRFS disk mount need physical access	7.8
spark	linux-libc-dev	CVE-2017-13165	LOW	5.4.0-166.183		escalation of privileges	7.8
ubuntu	perl-base	CVE-2020-12723	LOW	5.26.1-6ubuntu0.3	5.26.1-6ubuntu0.5	regular expression buffer overflow	7.5
ubuntu	libstdc++6	CVE-2019-15847	LOW	8.3.0-6ubuntu1~18.04.1	8.3.0-26ubuntu1~18.04	insufficient entropy	7.5
ubuntu	libpcre3	CVE-2019-20838	LOW	2:8.39-9	2:8.39-9ubuntu0.1	buffer over-read with UTF disabled	7.5
ubuntu	libgcrypt20	CVE-2021-33560	LOW	1.8.1-4ubuntu1.1	1.8.1-4ubuntu1.3	side channel attack confidentiality	7.5
ubuntu	libgcc1	CVE-2019-15847	LOW	1:8.3.0-6ubuntu1~18.04.1	8.3.0-26ubuntu1~18.04	insufficient entropy	7.5
ubuntu	libc6	CVE-2021-3326	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	assertion failure	7.5
ubuntu	libc-bin	CVE-2021-3326	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	assertion failure	7.5
ubuntu	gcc-8-base	CVE-2019-15847	LOW	8.3.0-6ubuntu1~18.04.1	8.3.0-26ubuntu1~18.04	insufficient entropy	7.5
spark	linux-libc-dev	CVE-2021-34981	LOW	5.4.0-166.183		privilege escalation	7.5
spark	linux-libc-dev	CVE-2019-19814	LOW	5.4.0-166.183		kernel leak and system crash	7.3
spark	libudev1	CVE-2023-26604	LOW	245.4-4ubuntu3.22		privilege escalation	7.1
spark	libsystemd0	CVE-2023-26604	LOW	245.4-4ubuntu3.22		privilege escalation	7.1
spark	libldap-common	CVE-2023-2953	LOW	2.4.49+dfsg-2ubuntu1.9		low impact null pointer dereference	7.1
spark	libldap-2.4-2	CVE-2023-2953	LOW	2.4.49+dfsg-2ubuntu1.9		low impact null pointer dereference	7.1
cassandra	libudev1	CVE-2023-26604	LOW	245.4-4ubuntu3.22		privilege escalation	7.1

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
cassandra	libsystemd0	CVE-2023-26604	LOW	245.4-4ubuntu3.22		privilege escalation	7.1
cassandra	libldap-common	CVE-2023-2953	LOW	2.4.49+dfsg-2ubuntu1.9		low impact null pointer dereference	7.1
cassandra	libldap-2.4-2	CVE-2023-2953	LOW	2.4.49+dfsg-2ubuntu1.9		low impact null pointer dereference	7.1
ubuntu	libc6	CVE-2022-23219	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service and code execution	7.0
ubuntu	libc6	CVE-2022-23218	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service and code execution	7.0
ubuntu	libc6	CVE-2020-1752	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	use-after-free	7.0
ubuntu	libc-bin	CVE-2022-23219	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service and code execution	7.0
ubuntu	libc-bin	CVE-2022-23218	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service and code execution	7.0
ubuntu	libc-bin	CVE-2020-1752	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	use-after-free	7.0
spark	linux-libc-dev	CVE-2023-1989	LOW	5.4.0-166.183		use-after-free	7.0
spark	linux-libc-dev	CVE-2022-45885	LOW	5.4.0-166.183		use-after-free	7.0
ubuntu	util-linux	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	mount	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libuuid1	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libsmartcols1	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libmount1	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libfdisk1	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libblkid1	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	fdisk	CVE-2018-7738	LOW	2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	bsdutils	CVE-2018-7738	LOW	1:2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	command injection	6.7
ubuntu	libgnutls30	CVE-2021-4209	LOW	3.5.18-1ubuntu1.2	3.5.18-1ubuntu1.6	pointer dereference	6.5
ubuntu	libc6	CVE-2019-9169	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	regular expression buffer over-read	6.5
ubuntu	libc-bin	CVE-2019-9169	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	regular expression buffer over-read	6.5
spark	linux-libc-dev	CVE-2023-33288	LOW	5.4.0-166.183		use-after-free	6.4
spark	linux-libc-dev	CVE-2022-45884	LOW	5.4.0-166.183		use-after-free	6.4
spark	linux-libc-dev	CVE-2022-44034	LOW	5.4.0-166.183		use-after-free	6.4
spark	linux-libc-dev	CVE-2022-44033	LOW	5.4.0-166.183		use-after-free	6.4
spark	gpgv	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gpgsm	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	gpgconf	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gpg-wks-server	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gpg-wks-client	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gpg-agent	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gpg	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gnupg2	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gnupg-utils	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gnupg-l10n	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	gnupg	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
spark	dirmngr	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
cassandra	github.com/opencontainers/runc	CVE-2023-25809	LOW	v1.1.0	1.1.5	local denial of service	6.3
cassandra	gpgv	CVE-2022-3219	LOW	2.2.19-3ubuntu2.2		denial of service	6.3
ubuntu	libgmp10	CVE-2021-43618	LOW	2:6.1.2+dfsg-2	2:6.1.2+dfsg-2ubuntu0.1	integer overflow crash	6.2
spark	coreutils	CVE-2016-2781	LOW	8.30-3ubuntu2		privilege bypass	6.2
cassandra	coreutils	CVE-2016-2781	LOW	8.30-3ubuntu2		privilege bypass	6.2
ubuntu	ncurses-bin	CVE-2022-29458	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	segmentation fault	6.1
ubuntu	ncurses-base	CVE-2022-29458	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	segmentation fault	6.1
ubuntu	libudev1	CVE-2020-13529	LOW	237-3ubuntu10.33	237-3ubuntu10.49	denial of service	6.1
ubuntu	libtinfo5	CVE-2022-29458	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	segmentation fault	6.1
ubuntu	libsystemd0	CVE-2020-13529	LOW	237-3ubuntu10.33	237-3ubuntu10.49	denial of service	6.1
ubuntu	libncursesw5	CVE-2022-29458	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	segmentation fault	6.1
ubuntu	libncurses5	CVE-2022-29458	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	segmentation fault	6.1
spark	locales	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	locales	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc6-dev	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc6-dev	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc6	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc6	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc-dev-bin	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	libc-dev-bin	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc-bin	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
spark	libc-bin	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	locales	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	locales	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	libc6	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	libc6	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	libc-bin	CVE-2023-4813	LOW	2.31-0ubuntu9.12		rare crash	5.9
cassandra	libc-bin	CVE-2023-4806	LOW	2.31-0ubuntu9.12		rare crash	5.9
ubuntu	libc6	CVE-2020-10029	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	stack overflow	5.7
ubuntu	libc-bin	CVE-2020-10029	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	stack overflow	5.7
ubuntu	tar	CVE-2021-20193	LOW	1.29b-2ubuntu0.1	1.29b-2ubuntu0.3	uncontrolled consumption of memory	5.5
ubuntu	tar	CVE-2018-20482	LOW	1.29b-2ubuntu0.1	1.29b-2ubuntu0.2	local denial of service	5.5
ubuntu	ncurses-bin	CVE-2021-39537	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap overflow	5.5
ubuntu	ncurses-base	CVE-2021-39537	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap overflow	5.5
ubuntu	libtinfo5	CVE-2021-39537	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap overflow	5.5
ubuntu	libncursesw5	CVE-2021-39537	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap overflow	5.5
ubuntu	libncurses5	CVE-2021-39537	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap overflow	5.5
ubuntu	libc6	CVE-2020-27618	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	infinite loop	5.5
ubuntu	libc-bin	CVE-2020-27618	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	infinite loop	5.5
spark	patch	CVE-2021-45261	LOW	2.7.6-6		crash or code execution	5.5
spark	passwd	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.4		social-engineered denial of service	5.5
spark	login	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.4		social-engineered denial of service	5.5
spark	linux-libc-dev	CVE-2023-4134	LOW	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2023-4133	LOW	5.4.0-166.183		denial of service	5.5
spark	linux-libc-dev	CVE-2023-31085	LOW	5.4.0-166.183	5.4.0-167.184	divide-by-zero	5.5
spark	linux-libc-dev	CVE-2022-0854	LOW	5.4.0-166.183		memory leak	5.5
spark	linux-libc-dev	CVE-2021-44879	LOW	5.4.0-166.183		pointer dereference	5.5
spark	linux-libc-dev	CVE-2020-12364	LOW	5.4.0-166.183		local denial of service	5.5

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	linux-libc-dev	CVE-2020-12363	LOW	5.4.0-166.183		local denial of service	5.5
spark	libpng16-16	CVE-2022-3857	LOW	1.6.37-2		segmentation fault	5.5
spark	libctf0	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
spark	libctf-nobfd0	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
spark	libbinutils	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
spark	binutils-x86-64-linux-gnu	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
spark	binutils-common	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
spark	binutils	CVE-2022-48064	LOW	2.34-6ubuntu1.6		denial of service	5.5
cassandra	passwd	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.4		social-engineered denial of service	5.5
cassandra	login	CVE-2023-29383	LOW	1:4.8.1-1ubuntu5.20.04.4		social-engineered denial of service	5.5
cassandra	libpng16-16	CVE-2022-3857	LOW	1.6.37-2		segmentation fault	5.5
ubuntu	ncurses-bin	CVE-2019-17595	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.4
ubuntu	ncurses-base	CVE-2019-17595	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.4
ubuntu	libtinfo5	CVE-2019-17595	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.4
ubuntu	libncursesw5	CVE-2019-17595	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.4
ubuntu	libncurses5	CVE-2019-17595	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.4
ubuntu	gpgv	CVE-2019-13050	LOW	2.2.4-1ubuntu1.2	2.2.4-1ubuntu1.5	cross site request forgery	5.4
ubuntu	libpcre3	CVE-2020-14155	LOW	2:8.39-9	2:8.39-9ubuntu0.1	integer overflow	5.3
ubuntu	libncurses5	CVE-2019-17594	LOW	6.1-1ubuntu1.18.04	6.1-1ubuntu1.18.04.1	heap-based buffer over-read	5.3
ubuntu	gpgv	CVE-2019-14855	LOW	2.2.4-1ubuntu1.2	2.2.4-1ubuntu1.3	certification forgery	5.3
spark	locales	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
spark	linux-libc-dev	CVE-2018-12928	LOW	5.4.0-166.183		denial of service	5.0
spark	libc6-dev	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
spark	libc6	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
spark	libc-dev-bin	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
spark	libc-bin	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
cassandra	locales	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
cassandra	libc6	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0
cassandra	libc-bin	CVE-2016-20013	LOW	2.31-0ubuntu9.12		denial of service	5.0

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
ubuntu	libc6	CVE-2020-29562	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service	4.8
ubuntu	libc6	CVE-2019-25013	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	segmentation fault	4.8
ubuntu	libc-bin	CVE-2020-29562	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service	4.8
ubuntu	libc-bin	CVE-2019-25013	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	segmentation fault	4.8
ubuntu	libhogweed4	CVE-2018-16869	LOW	3.4-1	3.4.1-0ubuntu0.18.04.1	Bleichenbacher type side-channel attack	4.7
spark	linux-libc-dev	CVE-2023-22995	LOW	5.4.0-166.183		local user crash	4.7
spark	linux-libc-dev	CVE-2017-0537	LOW	5.4.0-166.183		information disclosure	4.7
spark	libctf0	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	libctf-nobfd0	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	libbinutils	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	binutils-x86-64-linux-gnu	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	binutils-common	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	binutils	CVE-2019-1010204	LOW	2.34-6ubuntu1.6		denial of service	4.7
spark	linux-libc-dev	CVE-2018-12931	LOW	5.4.0-166.183		denial of service and possible privilege escalation	4.6
spark	linux-libc-dev	CVE-2018-12930	LOW	5.4.0-166.183		denial of service	4.6
spark	linux-libc-dev	CVE-2018-12929	LOW	5.4.0-166.183		denial of service	4.6
ubuntu	libudev1	CVE-2019-3844	LOW	237-3ubuntu10.33	237-3ubuntu10.38	privilege chaining	4.5
ubuntu	libudev1	CVE-2019-3843	LOW	237-3ubuntu10.33	237-3ubuntu10.38	incorrect privilege assignment	4.5
ubuntu	libsystemd0	CVE-2019-3844	LOW	237-3ubuntu10.33	237-3ubuntu10.38	privilege chaining	4.5
ubuntu	libsystemd0	CVE-2019-3843	LOW	237-3ubuntu10.33	237-3ubuntu10.38	incorrect privilege assignment	4.5
ubuntu	passwd	CVE-2018-7169	LOW	1:4.5-1ubuntu2	1:4.5-1ubuntu2.2	privilege dropping	4.4
ubuntu	login	CVE-2018-7169	LOW	1:4.5-1ubuntu2	1:4.5-1ubuntu2.2	privilege dropping	4.4
spark	passwd	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.4		time-of-check time-of-use race condition	4.4
spark	login	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.4		time-of-check time-of-use race condition	4.4
spark	linux-libc-dev	CVE-2020-14304	LOW	5.4.0-166.183		memory disclosure	4.4
cassandra	passwd	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.4		time-of-check time-of-use race condition	4.4
cassandra	login	CVE-2013-4235	LOW	1:4.8.1-1ubuntu5.20.04.4		time-of-check time-of-use race condition	4.4

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	linux-libc-dev	CVE-2019-15213	LOW	5.4.0-166.183		free-after-use crash	4.3
spark	linux-libc-dev	CVE-2022-41848	LOW	5.4.0-166.183		use-after-free	4.2
spark	linux-libc-dev	CVE-2018-1121	LOW	5.4.0-166.183		race condition	3.9
httpd-alpine	libcurl	CVE-2023-38546	LOW	7.88.1-r1	8.4.0-r0	cookie injection	3.7
httpd-alpine	libcurl	CVE-2023-28322	LOW	7.88.1-r1	8.1.0-r0	information leak	3.7
amazon-linux	libcurl	CVE-2023-38546	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	cookie injection	3.7
amazon-linux	curl	CVE-2023-38546	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	specific conditions needed for cookie injection risk of harm low	3.7
spark	linux-libc-dev	CVE-2020-35501	LOW	5.4.0-166.183		incorrect authorization	3.4
ubuntu	tar	CVE-2019-9923	LOW	1.29b-2ubuntu0.1	1.29b-2ubuntu0.2	pointer dereference	3.3
ubuntu	libsepol1	CVE-2021-36087	LOW	2.7-1	2.7-1ubuntu0.1	buffer over-read	3.3
ubuntu	libsepol1	CVE-2021-36086	LOW	2.7-1	2.7-1ubuntu0.1	use-after-free	3.3
ubuntu	libsepol1	CVE-2021-36085	LOW	2.7-1	2.7-1ubuntu0.1	use-after-free	3.3
ubuntu	libsepol1	CVE-2021-36084	LOW	2.7-1	2.7-1ubuntu0.1	use-after-free	3.3
ubuntu	libc6	CVE-2016-10228	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service	3.3
ubuntu	libc-bin	CVE-2016-10228	LOW	2.27-3ubuntu1	2.27-3ubuntu1.5	denial of service	3.3
spark	com.google.guava:guava	CVE-2020-8908	LOW	30.1.1-jre	32.0.0-android	information exposure	3.3
spark	com.google.guava:guava	CVE-2020-8908	LOW	30.1.1-jre	32.0.0-android	information exposure	3.3
spark	com.google.guava:guava	CVE-2020-8908	LOW	14.0.1	32.0.0-android	information exposure	3.3
spark	com.google.guava:guava	CVE-2020-8908	LOW	14.0.1	32.0.0-android	information exposure	3.3
spark	procps	CVE-2023-4016	LOW	2:3.3.16-1ubuntu2.3	2:3.3.16-1ubuntu2.4	denial of service	3.3
spark	patch	CVE-2018-6952	LOW	2.7.6-6		double free flaw	3.3
spark	linux-libc-dev	CVE-2017-13693	LOW	5.4.0-166.183		sensitive information leak	3.3
spark	libprocps8	CVE-2023-4016	LOW	2:3.3.16-1ubuntu2.3	2:3.3.16-1ubuntu2.4	denial of service	3.3
spark	libpcre3	CVE-2017-11164	LOW	2:8.39-12ubuntu0.1		uncontrolled recursion	3.3
spark	libctf0	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	libctf0	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	libctf-nobfd0	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	libctf-nobfd0	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification	CVSS
spark	libbinutils	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	libbinutils	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils-x86-64-linux-gnu	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils-x86-64-linux-gnu	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils-common	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils-common	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils	CVE-2018-20657	LOW	2.34-6ubuntu1.6		denial of service	3.3
spark	binutils	CVE-2017-13716	LOW	2.34-6ubuntu1.6		denial of service	3.3
cassandra	com.google.guava:guava	CVE-2020-8908	LOW	27.0-jre	32.0.0-android	information exposure	3.3
cassandra	procps	CVE-2023-4016	LOW	2:3.3.16-1ubuntu2.3	2:3.3.16-1ubuntu2.4	denial of service	3.3
cassandra	libprocps8	CVE-2023-4016	LOW	2:3.3.16-1ubuntu2.3	2:3.3.16-1ubuntu2.4	denial of service	3.3
cassandra	libpcre3	CVE-2017-11164	LOW	2:8.39-12ubuntu0.1		uncontrolled recursion	3.3
ubuntu	libc6	CVE-2019-19126	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	improper input validation	2.9
ubuntu	libc-bin	CVE-2019-19126	LOW	2.27-3ubuntu1	2.27-3ubuntu1.2	improper input validation	2.9
spark	org.eclipse.jetty:jetty-http	CVE-2022-2047	LOW	9.4.43.v20210629	9.4.47, 10.0.10, 11.0.10	faliure in proxy not exploitable	2.7
ubuntu	libudev1	CVE-2019-20386	LOW	237-3ubuntu10.33	237-3ubuntu10.38	memory leak	2.4
ubuntu	libsystemd0	CVE-2019-20386	LOW	237-3ubuntu10.33	237-3ubuntu10.38	memory leak	2.4
amazon-linux	ca-certificates	CVE-2023-37920	HIGH	2021.2.50-72.amzn2.0.7	2021.2.50-72.amzn2.0.8	certificates have been removed as of 07.22.2023	0.0
spark	org.eclipse.jetty:jetty-xml	GHSA-58qw-p7qm-5rvh	LOW	9.4.43.v20210629	10.0.16, 11.0.16, 12.0.0, 9.4.52	attacker would already have access	N/A

4. Remediation Plan

4.1 Action Items

Cassandra requires an upgrade to the latest patched version for optimal security. Authentication and access controls should be enabled to restrict unauthorized access. TLS should be configured for encryption in transit to safeguard sensitive data. For Amazon Linux, applying the latest OS security patches is crucial. Unnecessary services should be disabled to improve security posture. Audit logging and monitoring should be enabled to track and investigate suspicious activities. Httpd-alpine requires an upgrade to the latest patched version for optimal security and firewall and configuration rules should be written for spark. The scans illustrate the importance of remaining up to date as many vulnerabilities could be solved with proper patch management.

Asset	Package	Action Items
cassandra	org.yaml:snakeyaml	adopt a secure by default policy and replace use of snakeyaml's Constructor() class with SafeConstructor()
ubuntu	libudev1	update to 237-3ubuntu10.56 as this bug has been fixed
ubuntu	libsystemd0	update to 237-3ubuntu10.56 as this bug has been fixed
spark	org.apache.derby:derby	Users should upgrade to Java 21 and Derby 10.17.1.0 or Java LTS versions 17, 11, and 8 and Build Derby from backported versions 10.16, 10.15, and 10.14
ubuntu	dpkg	update to version 1.21.8, 1.20.10, 1.19.8, 1.18.26 or newer
spark	org.apache.zookeeper:zookeeper	upgrade to version 3.9.1, 3.8.3, 3.7.2, which fixes the issue and/or ensure election/qourum communication is protected by a firewall
ubuntu	gzip	update to 1.6-5ubuntu1.2 no other mitigation available
cassandra	python3.8	upgrade to Python 3.11.5, 3.10.13, 3.9.18, or 3.8.18
cassandra	python3.8-minimal	upgrade to Python 3.11.5, 3.10.13, 3.9.18, or 3.8.18
cassandra	libpython3.8-stdlib	upgrade to Python 3.11.5, 3.10.13, 3.9.18, or 3.8.18
cassandra	libpython3.8-minimal	upgrade to Python 3.11.5, 3.10.13, 3.9.18, or 3.8.18
spark	org.apache.ivy:ivy	upgrade to ivy version 2.5.2 and ensure DTD processing is disabled by default
httpd-alpine	libcurl	set CURLOPT_BUFFERSIZE to be larger that 65kB or do not use 'CURLPROXY_SOCKS5_HOSTNAME' proxies with curl. Also do not set a proxy environment variable to socks5h://
spark	org.codehaus.jackson:jackson-mapper-asl	implement a whitelist approach to mitigate this vulnerability and similar one in the future
amazon-linux	libcurl	set CURLOPT_BUFFERSIZE to be larger that 65kB or do not use 'CURLPROXY_SOCKS5_HOSTNAME' proxies with curl. Also do not set a proxy environment variable to socks5h://
amazon-linux	curl	set CURLOPT_BUFFERSIZE to be larger that 65kB or do not use 'CURLPROXY_SOCKS5_HOSTNAME' proxies with curl. Also do not set a proxy environment variable to socks5h://

4.2 Responsible Teams

Action Item	Patch Management Team	Network Security Team	Application Security Team
Review patch contents	A	I	I
Test patches	R	I	I
Approve patches	I	I	C
Deploy patches	R	I	I
Configure Network Security	I	R	I
Monitor systems	I	R	A
Respond to issues	C	I	R