Vulnerability Remediation Plan Template

1. Asset Identification and Documentation

1.1 Asset Inventory

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

2. Prioritization of Assets

Prioritize assets based on their criticality to business functions and potential impact on the enterprise in case of a security breach.

- 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
- Medium Priority Assets:
  - httpd-alpine due to impact on availability and scheduling

3. Prioritization of Vulnerabilities

Rank vulnerabilities based on their severity, potential impact, and exploitability. Also consider the asset prioritization when ranking vulnerabilities. Make note of any assumptions made.

3.1 Critical Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
org.apache.zookeeper:zookeeper	CVE-2023-44981	CRITICAL	3.6.3	3.7.2, 3.8.3, 3.9.1	
org.codehaus.jackson:jackson-mapper-asl	CVE-2019-10202	CRITICAL	1.9.13		
org.apache.derby:derby	CVE-2022-46337	CRITICAL	10.14.2.0	10.17.1.0	
libcurl	CVE-2023-38545	CRITICAL	7.88.1-r1	8.4.0-r0	

3.2 High-Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
gback:logback-classic	CVE-2023-6378	HIGH	1.2.9	1.3.12, 1.4.12	
gback:logback-core	CVE-2023-6378	HIGH	1.2.9	1.3.12, 1.4.12	
erxml.jackson.core:jackson-l	CVE-2022-42003	HIGH	2.13.2.2	2.12.7.1, 2.13.4.2	
erxml.jackson.core:jackson-l	CVE-2022-42004	HIGH	2.13.2.2	2.12.7.1, 2.13.4	
l.snappy:snappy-java	CVE-2023-43642	HIGH	1.1.10.1	1.1.10.4	
:snakeyaml	CVE-2022-1471	HIGH	1.26	2.0	
:snakeyaml	CVE-2022-25857	HIGH	1.26	1.31	
om/opencontainers/runc	CVE-2023-27561	HIGH	v1.1.0	1.1.5	
he.ivy:ivy	CVE-2022-46751	HIGH	2.5.1	2.5.2	
he.mesos:mesos	CVE-2018-1330	HIGH	1.4.3	1.6.0	
he.thrift:libthrift	CVE-2019-0205	HIGH	0.12.0	0.13.0	
he.thrift:libthrift	CVE-2020-13949	HIGH	0.12.0	0.14.0	
haus.jackson:jackson-asl	CVE-2019-10172	HIGH	1.9.13		
l.snappy:snappy-java	CVE-2023-43642	HIGH	1.1.10.3	1.1.10.4	
he.avro:avro	CVE-2023-39410	HIGH	1.7.7	1.11.3	
he.avro:avro	CVE-2023-39410	HIGH	1.11.2	1.11.3	
dev:json-smart	CVE-2023-1370	HIGH	1.3.2	2.4.9	
dev:json-smart	CVE-2021-31684	HIGH	1.3.2	1.3.3, 2.4.4	
etty-codec-http2	GHSA-xpw8-rcwv-8f8p	HIGH	4.1.96.Final	4.1.100.Final	

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
gle.protobuf:protobuf-java	CVE-2022-3510	HIGH	3.7.1	3.16.3, 3.19.6, 3.20.3, 3.21.7	
gle.protobuf:protobuf-java	CVE-2022-3509	HIGH	3.7.1	3.16.3, 3.19.6, 3.20.3, 3.21.7	
gle.protobuf:protobuf-java	CVE-2021-22570	HIGH	3.7.1	3.15.0	
gle.protobuf:protobuf-java	CVE-2021-22569	HIGH	3.7.1	3.16.1, 3.18.2, 3.19.2	
gle.protobuf:protobuf-java	CVE-2022-3510	HIGH	3.3.0	3.16.3, 3.19.6, 3.20.3, 3.21.7	
gle.protobuf:protobuf-java	CVE-2022-3509	HIGH	3.3.0	3.16.3, 3.19.6, 3.20.3, 3.21.7	
gle.protobuf:protobuf-java	CVE-2021-22570	HIGH	3.3.0	3.15.0	
gle.protobuf:protobuf-java	CVE-2021-22569	HIGH	3.3.0	3.16.1, 3.18.2, 3.19.2	
gle.code.gson:gson	CVE-2022-25647	HIGH	2.2.4	2.8.9	
erxml.jackson.core:jackson-l	CVE-2022-42004	HIGH	2.12.7	2.12.7.1, 2.13.4	
erxml.jackson.core:jackson-l	CVE-2022-42003	HIGH	2.12.7	2.12.7.1, 2.13.4.2	
:-dev	CVE-2023-4244	HIGH	5.4.0-166.183		
:-dev	CVE-2023-20569	HIGH	5.4.0-166.183		
cates	CVE-2023-37920	HIGH	2021.2.50-72.amzn2.0.7	2021.2.50-72.amzn2.0.8	
	CVE-2023-38039	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.1	
	CVE-2023-38545	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	
	CVE-2023-38546	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	
	CVE-2023-38039	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.1	
	CVE-2023-38545	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	
	CVE-2023-38546	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.4	

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
2	CVE-2023-44487	HIGH	1.41.0-1.amzn2.0.1	1.41.0-1.amzn2.0.4	
	CVE-2020-22218	HIGH	1.4.3-12.amzn2.2.4	1.4.3-12.amzn2.2.6	
	CVE-2023-45322	HIGH	2.9.1-6.amzn2.5.8	2.9.1-6.amzn2.5.13	
	CVE-2022-48565	HIGH	2.7.18-1.amzn2.0.6	2.7.18-1.amzn2.0.7	
bs	CVE-2022-48565	HIGH	2.7.18-1.amzn2.0.6	2.7.18-1.amzn2.0.7	
	CVE-2021-3236	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4733	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4734	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4735	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4738	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4750	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4751	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4752	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
	CVE-2023-4781	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2021-3236	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4733	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4734	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4735	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4738	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4750	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
mal	CVE-2023-4751	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4752	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
mal	CVE-2023-4781	HIGH	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	
nd0	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	
	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	
3	CVE-2023-5363	HIGH	3.0.8-r3	3.0.12-r0	
	CVE-2023-28319	HIGH	7.88.1-r1	8.1.0-r0	
	CVE-2023-38039	HIGH	7.88.1-r1	8.3.0	
	CVE-2023-5363	HIGH	3.0.8-r3	3.0.12-r0	
libs	CVE-2023-35945	HIGH	1.51.0-r0	1.51.0-r1	
libs	CVE-2023-44487	HIGH	1.51.0-r0	1.51.0-r2	
	CVE-2023-47038	HIGH	5.36.0-r0	5.36.2-r0	

3.3 Medium-Priority Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Ver
cassandra	libc-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu
cassandra	libc6	CVE-2023-5156	MEDIUM	2.31-0ubuntu
cassandra	libgnutls30	CVE-2023-5981	MEDIUM	3.6.13-2ubuntu1.8
cassandra	libgssapi-krb5-2	CVE-2023-36054	MEDIUM	1.17-6ubuntu
cassandra	libk5crypto3	CVE-2023-36054	MEDIUM	1.17-6ubuntu
cassandra	libkrb5-3	CVE-2023-36054	MEDIUM	1.17-6ubuntu
cassandra	libkrb5support0	CVE-2023-36054	MEDIUM	1.17-6ubuntu
cassandra	liblzma5	CVE-2020-22916	MEDIUM	5.2.4-1ubuntu
cassandra	libnghttp2-14	CVE-2023-44487	MEDIUM	1.40.0-1ubuntu0.1
cassandra	libpython3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20
cassandra	libpython3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20
cassandra	libpython3.8-stdlib	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20
cassandra	libpython3.8-stdlib	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20
cassandra	locales	CVE-2023-5156	MEDIUM	2.31-0ubuntu
cassandra	perl-base	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4
cassandra	python3.8	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20
cassandra	python3.8	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20
cassandra	python3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20
cassandra	python3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20

Asset	Package	Vulnerability ID	Severity	Installed Ver
cassandra	tar	CVE-2023-39804	MEDIUM	1.30+dfsg-7ubuntu0.20.
cassandra	wget	CVE-2021-31879	MEDIUM	1.20.3-1ubun
cassandra	com.google.guava:guava	CVE-2023-2976	MEDIUM	27.0-jre
cassandra	org.yaml:snakeyaml	CVE-2022-38749	MEDIUM	1.26
cassandra	org.yaml:snakeyaml	CVE-2022-38750	MEDIUM	1.26
cassandra	org.yaml:snakeyaml	CVE-2022-38751	MEDIUM	1.26
cassandra	org.yaml:snakeyaml	CVE-2022-38752	MEDIUM	1.26
cassandra	org.yaml:snakeyaml	CVE-2022-41854	MEDIUM	1.26
cassandra	github.com/opencontainers/runc	CVE-2022-29162	MEDIUM	v1.1.0
cassandra	github.com/opencontainers/runc	CVE-2023-28642	MEDIUM	v1.1.0
amazon-linux	curl	CVE-2020-19909	MEDIUM	8.0.1-1.amzn
amazon-linux	curl	CVE-2023-28319	MEDIUM	8.0.1-1.amzn
amazon-linux	curl	CVE-2023-28321	MEDIUM	8.0.1-1.amzn
amazon-linux	curl	CVE-2023-28322	MEDIUM	8.0.1-1.amzn
amazon-linux	elfutils-libelf	CVE-2020-21047	MEDIUM	0.176-2.amzr
amazon-linux	expat	CVE-2022-23990	MEDIUM	2.1.0-15.amzn2.0.2
amazon-linux	expat	CVE-2022-25313	MEDIUM	2.1.0-15.amzn2.0.2
amazon-linux	krb5-libs	CVE-2023-36054	MEDIUM	1.15.1-55.amzn2.2.5
amazon-linux	libcurl	CVE-2020-19909	MEDIUM	8.0.1-1.amzn
amazon-linux	libcurl	CVE-2023-28319	MEDIUM	8.0.1-1.amzn

Asset	Package	Vulnerability ID	Severity	Installed Ver
amazon-linux	libcurl	CVE-2023-28321	MEDIUM	8.0.1-1.amzn
amazon-linux	libcurl	CVE-2023-28322	MEDIUM	8.0.1-1.amzn
amazon-linux	libgcc	CVE-2023-4039	MEDIUM	7.3.1-15.amz
amazon-linux	libsepol	CVE-2021-36084	MEDIUM	2.5-8.1.amzn
amazon-linux	libsepol	CVE-2021-36085	MEDIUM	2.5-8.1.amzn
amazon-linux	libsepol	CVE-2021-36086	MEDIUM	2.5-8.1.amzn
amazon-linux	libsepol	CVE-2021-36087	MEDIUM	2.5-8.1.amzn
amazon-linux	libstdc++	CVE-2023-4039	MEDIUM	7.3.1-15.amz
amazon-linux	libxml2	CVE-2023-39615	MEDIUM	2.9.1-6.amzn
amazon-linux	openssl-libs	CVE-2023-3446	MEDIUM	1:1.0.2k-24.amzn2.0.7
amazon-linux	openssl-libs	CVE-2023-3817	MEDIUM	1:1.0.2k-24.amzn2.0.7
amazon-linux	vim-data	CVE-2023-46246	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-data	CVE-2023-5344	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-data	CVE-2023-5441	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-data	CVE-2023-5535	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-minimal	CVE-2023-46246	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-minimal	CVE-2023-5344	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-minimal	CVE-2023-5441	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	vim-minimal	CVE-2023-5535	MEDIUM	2:9.0.1592-1.amzn2.0.1
amazon-linux	zlib	CVE-2023-45853	MEDIUM	1.2.7-19.amzn2.0.2

Asset	Package	Vulnerability ID	Severity	Installed Ver
ubuntu	apt	CVE-2020-27350	MEDIUM	1.6.12
ubuntu	apt	CVE-2020-3810	MEDIUM	1.6.12
ubuntu	dpkg	CVE-2022-1664	MEDIUM	1.19.0.5ubun
ubuntu	e2fsprogs	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	e2fsprogs	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	gpgv	CVE-2022-34903	MEDIUM	2.2.4-1ubunt
ubuntu	gzip	CVE-2022-1271	MEDIUM	1.6-5ubuntu1
ubuntu	libapt-pkg5.0	CVE-2020-27350	MEDIUM	1.6.12
ubuntu	libapt-pkg5.0	CVE-2020-3810	MEDIUM	1.6.12
ubuntu	libc-bin	CVE-2018-11236	MEDIUM	2.27-3ubuntu
ubuntu	libc-bin	CVE-2018-11237	MEDIUM	2.27-3ubuntu
ubuntu	libc-bin	CVE-2018-19591	MEDIUM	2.27-3ubuntu
ubuntu	libc-bin	CVE-2020-1751	MEDIUM	2.27-3ubuntu
ubuntu	libc-bin	CVE-2021-3999	MEDIUM	2.27-3ubuntu
ubuntu	libc6	CVE-2018-11236	MEDIUM	2.27-3ubuntu
ubuntu	libc6	CVE-2018-11237	MEDIUM	2.27-3ubuntu
ubuntu	libc6	CVE-2018-19591	MEDIUM	2.27-3ubuntu
ubuntu	libc6	CVE-2020-1751	MEDIUM	2.27-3ubuntu
ubuntu	libc6	CVE-2021-3999	MEDIUM	2.27-3ubuntu
ubuntu	libcom-err2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2

Asset	Package	Vulnerability ID	Severity	Installed Ve
ubuntu	libcom-err2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	libext2fs2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	libext2fs2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	libgcrypt20	CVE-2019-13627	MEDIUM	1.8.1-4ubunt
ubuntu	libgcrypt20	CVE-2021-40528	MEDIUM	1.8.1-4ubunt
ubuntu	libgnutls30	CVE-2022-2509	MEDIUM	3.5.18-1ubuntu1.2
ubuntu	libhogweed4	CVE-2021-20305	MEDIUM	3.4-1
ubuntu	libhogweed4	CVE-2021-3580	MEDIUM	3.4-1
ubuntu	liblz4-1	CVE-2021-3520	MEDIUM	0.0~r131-2ubuntu3
ubuntu	liblzma5	CVE-2022-1271	MEDIUM	5.2.2-1.3
ubuntu	libncurses5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18
ubuntu	libncursesw5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18
ubuntu	libnettle6	CVE-2021-20305	MEDIUM	3.4-1
ubuntu	libnettle6	CVE-2021-3580	MEDIUM	3.4-1
ubuntu	libp11-kit0	CVE-2020-29361	MEDIUM	0.23.9-2
ubuntu	libp11-kit0	CVE-2020-29362	MEDIUM	0.23.9-2
ubuntu	libp11-kit0	CVE-2020-29363	MEDIUM	0.23.9-2
ubuntu	libss2	CVE-2019-5188	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	libss2	CVE-2022-1304	MEDIUM	1.44.1-1ubuntu1.2
ubuntu	libsystemd0	CVE-2020-1712	MEDIUM	237-3ubuntu10.3

Asset	Package	Vulnerability ID	Severity	Installed Ver
ubuntu	libsystemd0	CVE-2022-2526	MEDIUM	237-3ubuntu10.3
ubuntu	libsystemd0	CVE-2022-3821	MEDIUM	237-3ubuntu10.3
ubuntu	libtinfo5	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.
ubuntu	libudev1	CVE-2020-1712	MEDIUM	237-3ubuntu10.3
ubuntu	libudev1	CVE-2022-2526	MEDIUM	237-3ubuntu10.3
ubuntu	libudev1	CVE-2022-3821	MEDIUM	237-3ubuntu10.3
ubuntu	libzstd1	CVE-2021-24031	MEDIUM	1.3.3+dfsg-2ubuntu1.1
ubuntu	libzstd1	CVE-2021-24032	MEDIUM	1.3.3+dfsg-2ubuntu1.1
ubuntu	ncurses-base	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.
ubuntu	ncurses-bin	CVE-2023-29491	MEDIUM	6.1-1ubuntu1.18.
ubuntu	perl-base	CVE-2020-16156	MEDIUM	5.26.1-6ubuntu0.3
ubuntu	perl-base	CVE-2023-31484	MEDIUM	5.26.1-6ubuntu0.3
ubuntu	tar	CVE-2022-48303	MEDIUM	1.29b-2ubunt
ubuntu	zlib1g	CVE-2018-25032	MEDIUM	1:1.2.11.dfsg-0ubuntu2
ubuntu	zlib1g	CVE-2022-37434	MEDIUM	1:1.2.11.dfsg-0ubuntu2
binutils	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	

Asset	Package	Vulnerability ID	Severity	Installed Ver
binutils	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
binutils	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
binutils-common	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	

Asset	Package	Vulnerability ID	Severity	Installed Ver
binutils-x86-64-linux-gnu	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
binutils-x86-64-linux-gnu	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
cpp	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2	
g++	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2	
gcc	CVE-2020-13844	MEDIUM	4:9.3.0-1ubuntu2	
krb5-user	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libbinutils	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
libbinutils	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
libc-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12	
libc-dev-bin	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12	
libc6	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12	
libc6-dev	CVE-2023-5156	MEDIUM	2.31-0ubuntu9.12	
libctf-nobfd0	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	

Asset	Package	Vulnerability ID	Severity	Installed Ver
libctf-nobfd0	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
libctf-nobfd0	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2020-19726	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2021-46174	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-35205	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-44840	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-45703	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-47007	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-47008	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-47010	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-47011	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-47695	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-48063	MEDIUM	2.34-6ubuntu1.6	
libctf0	CVE-2022-48065	MEDIUM	2.34-6ubuntu1.6	
libgnutls30	CVE-2023-5981	MEDIUM	3.6.13-2ubuntu1.8	3.6.13-2ubuntu1.9
libgssapi-krb5-2	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libgssrpc4	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libk5crypto3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libkadm5clnt-mit11	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libkadm5srv-mit11	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libkdb5-9	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libkrb5-3	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
libkrb5support0	CVE-2023-36054	MEDIUM	1.17-6ubuntu4.3	1.17-6ubuntu
liblzma5	CVE-2020-22916	MEDIUM	5.2.4-1ubuntu1.1	

Asset	Package	Vulnerability ID	Severity	Installed Ver
libnghttp2-14	CVE-2023-44487	MEDIUM	1.40.0-1ubuntu0.1	1.40.0-1ubuntu0.2
libnss3	CVE-2023-4421	MEDIUM	2:3.49.1-1ubuntu1.9	
libnss3	CVE-2023-5388	MEDIUM	2:3.49.1-1ubuntu1.9	
libperl5.30	CVE-2023-47038	MEDIUM	5.30.0-9ubuntu0.4	5.30.0-9ubuntu0.5
libpython3.8	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8	
libpython3.8	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20
libpython3.8-dev	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8	
libpython3.8-dev	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20
libpython3.8-minimal	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8	
libpython3.8-minimal	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20
libpython3.8-stdlib	CVE-2023-27043	MEDIUM	3.8.10-0ubuntu1~20.04.8	
libpython3.8-stdlib	CVE-2023-40217	MEDIUM	3.8.10-0ubuntu1~20.04.8	3.8.10-0ubuntu1~20
linux-libc-dev	CVE-2013-7445	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2015-8553	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2016-8660	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2018-17977	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2020-12362	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2020-24504	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2020-26144	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2020-27835	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2020-36310	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2021-3864	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2021-4148	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-0400	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-0480	MEDIUM	5.4.0-166.183	

Asset	Package	Vulnerability ID	Severity	Installed Ver
linux-libc-dev	CVE-2022-1247	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-1280	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-25836	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-2961	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-29900	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-3344	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-3523	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-36402	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-38096	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-38457	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-39189	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-40133	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2022-4543	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-0030	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-1582	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-2007	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-23000	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-23004	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-26242	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-28327	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-3006	MEDIUM	5.4.0-166.183	
linux-libc-dev	CVE-2023-31082	MEDIUM	5.4.0-166.183	

3.4 Low-Priority Vulnerabilities

Asset	Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification

4. Remediation Plan

4.1 Action Items

Outline specific actions to remediate each critical vulnerability. Include details such as patching, configuration changes, or deployment of additional security measures. Asset Package Action Items

4.2 Responsible Teams

Identify the teams responsible for executing each action item. USE A RACI TABLE Patch Management Team: [Specify responsibilities] Network Security Team: [Specify responsibilities] Application Security Team: [Specify responsibilities]