Asset Identification and Documentation

Asset Inventory:
Asset Name: EHR System
Type: Application
Owner: IT Department
Function: Electronic Health Record (EHR) system for storing and managing patient health records, including medical history, diagnoses, medications, and treatment plans.
Dental Imaging System:

Asset Name: Dental Imaging System
Type: Application
Owner: Radiology Department
Function: Software used for capturing, storing, and viewing dental imaging data, including X-rays, CT scans, and intraoral photographs, to aid diagnosis and treatment planning.
Amazon EC2 Archiving Server:

Asset Name: Amazon EC2 Archiving Server
Type: Server
Owner: IT Infrastructure Team
Function: Server instance running on Amazon EC2 used for archiving and storing backup data, logs, and historical records in a secure and scalable cloud environment.

Priortirization Of Asset

Critical Asset	Priority	Justification
Electronic Health Records (EHR) System	High	This is based on the type of information it collects, processes, and stores, information such as Health information, treatment plan
Dental Imaging System	High	This is based on the type of information it collects, processes, and stores, information such as Patient records, treatment plan
Front Desk Endpoints	Medium	They do not not directly store sensitive patient data however, they facilitate access to crucial systems like the EHR
Cybersecurity Technologies	Medium	These are essential for protecting the integrity and confidentiality of patient data, but they do not store patient data directly.
Cloud-Based Systems(Amazon EC2 Archiving Server)	High	The primary function is to support data resilience and disaster recovery rather than directly storing sensitive patient information

Prioritization Of Vulnerability

EHR System: High-Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
libcrypto3	CVE-2023-5363	HIGH	3.0.8-r3	3.0.12-r0	This vulnerability could lead to potential loss of confidentiality for encrypted data (depending on specific use case)
nghttp2-libs	CVE-2023-44487	HIGH	1.51.0-r0	1.51.0-r2	The vulnerability that exists can be used by malicious actors can exploit this flaw to crash web servers with a massive flood of requests.
com.google.code.gson:gson	CVE-2022-25647	HIGH	2.2.4	2.8.9	Malicious code execution leading to Denial of service
org.apache.zookeeper:zookeeper	CVE-2023-44981	CRITICAL	3.6.3	3.7.2, 3.8.3, 3.9.1	This vulnerability could lead to unauthorized modification of sensitive information, security breaches, and Service disruption

EHR System: Medium Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
libcrypto3	CVE-2023-1255	MEDIUM	3.0.8-r3	3.0.8-r4	It compromises Confidentiality, Integrity, and Availability by potentially exposing data, altering files, or crashing the application. This vulnerability is easy to exploit.
libcurl	CVE-2023-28320	MEDIUM	7.88.1-r1	8.1.0-r0	It affects the OpenSSL Library which is highly used and if exploited, it could lead to full system compromise.

EHR System: low Priority Vulnerabilities

libcurl	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
libcurl	7	LOW	7.88.1-r1	8.1.0-r0	This is considered low because it doesn't allow for complete control of the system or cause severe damage. however, it can potentially reveal some sensitive information.
libcurl	CVE-2023-38546	LOW	7.88.1-r1	8.4.0-r0	Exploiting this vulnerability requires a specific set of conditions to be met and the condition is difficult to be met. if the condition is met, it might not lead to a major compromise.

Dental Imaging System: High-Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
libsystemd0	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	If attackers gain access, they can execute code to steal data or spy on Activities.
libudev1	CVE-2021-33910	HIGH	237-3ubuntu10.33	237-3ubuntu10.49	If this vulnerability is exploited, they can crash the entire operating system which can lead to Denial of service.

Dental Imaging System: Medium-Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
apt	CVE-2020-27350	MEDIUM	1.6.12	1.6.12ubuntu0.2	Exploiting this will make it difficult or impossible to install or update the software

libc-bin	CVE-2018-11236	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	This Vulnerability should be considered high because if the vulnerability is exploited, it can lead to malware infestation, theft of sensitive data, or Disruption of systems operations
libc6	CVE-2018-11236	MEDIUM	2.27-3ubuntu1	2.27-3ubuntu1.2	An attacker could potentially gain complete control of an affected system if exploited successfully.
zlib1g	CVE-2022-37434	MEDIUM	1:1.2.11.dfsg-0ubuntu2	1:1.2.11.dfsg-0ubuntu2.2	It doesn't allow an attacker to directly take control of the system or steal data, it can disrupt operations.

Dental Imaging System: Low-Priority Vulnerabilities

Package	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
bsdutils	CVE-2018-7738	Low	1:2.31.1-0.4ubuntu3.4	2.31.1-0.4ubuntu3.7	It requires local access and a specific set of circumstances for exploitation.
libc6	CVE-2016-10228	Low	2.27-3ubuntu1	2.27-3ubuntu1.5	It doesn't allow an attacker to directly take control of the system or steal data. However, it can cause a denial of service which can be disruptive.

Amazon EC2 Archiving Server: High-Priority Vulnerabilities

Packages	Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
libcurl	CVE-2023-38039	HIGH	8.0.1-1.amzn2.0.1	8.3.0-1.amzn2.0.1	a malicious server could send an endless stream of headers, causing curl to allocate a large amount of memory on the heap until the system runs out of resources and crashes.

ca-certificates	CVE-2023-37920	HIGH	2021.2.50-72.amzn2.0.7	2021.2.50-72.amzn2.0.8	The vulnerability existed in Certifi by adding untrusted e-tugra to certifi list leading to intercepting encrypted traffic and spoofing websites
Python	CVE-2022-48565	HIGH	2.7.18-1.amzn2.0.6	2.7.18-1.amzn2.0.7	This vulnerability is found in Python versions up to 3.9.1. the vulnerability can take advantage of how the module handles external entities, which can lead to the disclosure of sensitive information, Launch Denial-of-Service (DoS) attacks by exhausting resources, and potentially performing Server-side request forgery.

Amazon EC2 Archiving Server: Medinum-Priority Vulnerabilities

Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
CVE-2020-19909	MEDIUM	8.0.1-1.amzn2.0.1	8.2.1-1.amzn2.0.2	An integer overflow can cause unexpected behavior in the program and could potentially lead to Denial of service and unexpected program
CVE-2021-36084	MEDIUM	2.5-8.1.amzn2.0.2	2.5-10.amzn2.0.1	The vulnerability can be exploited to obtain higher privileges on the system and cause security policy manipulation.
CVE-2023-3446	MEDIUM	1:1.0.2k-24.amzn2.0.7	1:1.0.2k-24.amzn2.0.9	It doesn't allow attackers to steal data or compromise the system directly. However, it can be disruptive if exploited successfully.

Amazon EC2 Archiving Server: low-Priority Vulnerabilities

Vulnerability ID	Severity	Installed Version	Fixed Version	Justification
CVE-2023-4733	Low	2:9.0.1592-1.amzn2.0.1	2:9.0.1882-1.amzn2.0.1	It requires a local attacker to have an account on the system, the impact of exploiting the vulnerability is low

Remediation Plan

4.1 Action Items

Asset	Package	Action Items
EHR	org.apache.zookeeper:zookeeper	Update to a version(3.9.1, 3.8.3, or 3.7.2), temporarily set a firewall rule to restrict communication channels used for ZooKeeper's ensemble election process for CVE-2023-44981.
EHR	libcrypto3	Update OpenSSL for CVE-2023-5363
EHR	nghttp2-libs	
EHR	com.google.code.gson:gson	Update Gson to version 2.8.9 or later, temporarily implementing measures to sanitize user-provided JSON data before processing it with Gson for .
Dental Imaging System	libsystemd0	Update systemd to 237-3ubuntu10.49 to address the vulnerabilty for CVE-2021-33910
Dental Imaging System	libudev1	Update systemd to 237-3ubuntu10.49 to address the vulnerabilty for CVE-2021-33910
Amazon EC2 Archiving Server:	libcurl	Update curl in Linux macOS and Windows systems for CVE-2023-38039
Amazon EC2 Archiving Server:	ca-certificates	update Certifi to version 2023.07.22 for CVE-2023-37920
Amazon EC2 Archiving Server:	Python	Upgrading to Python version 3.9.2 or later, Disabling external entities processing in the plistlib library If immediate update is not possible for CVE-2022-48565

4.2 Responsible Teams

Here is a breakdown of the responsible teams for each action item based on typical organizational roles:

Electronic Health Record (EHR) System

1. Org.apache.zookeeper: zookeeper
   Responsible Team: Middleware/Infrastructure Team
2. libcrypto3
   - Responsible Team: Security/Infrastructure Team
3. nghttp2-libs
   Responsible Team: DevOps/Application Team
4. com.google.code.gson:gson
   Responsible Team: Application Development Team

Dental Imaging System

1. libsystemd0
   Responsible Team: Linux/Systems Administration Team
   Action: Update systemd to version 237-3ubuntu10.49.
2. libudev1
   Responsible Team: Linux/Systems Administration Team

Amazon EC2 Archiving Server

1. libcurl
   Responsible Team: DevOps/Systems Administration Team
2. ca-certificates
   Responsible Team: DevOps/Systems Administration Team
3. python
   Responsible Team: DevOps/Application Development Team