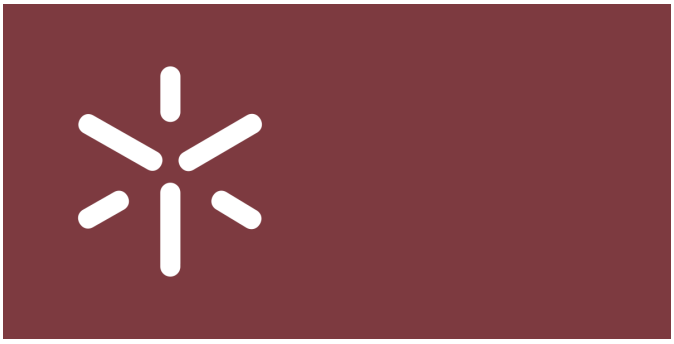


Universidade do Minho

Mestrado em Engenharia Informática

Tecnologias de Segurança

Trabalho Prático 2 - Grupo 11

A74806 - João Amorim

20 de Abril de 2024

Índice

Lista de Figuras

1 Introducão

1.1 Contextualização

No âmbito deste trabalho prático, propõe-se realizar uma análise de segurança de um sistema de suporte a interoperabilidade segura de dados médicos por meio da modelação de ameaças, utilizando o modelo STRIDE, assim como efetuar uma catalogação de vulnerabilidades e exploits presentes nas ferramentas do sistema. Esta análise será aplicada às várias Entidades do Sistema e às suas interações, sendo que a Modelação de Ameaças será feita à Aplicação do Paciente, à Aplicação Médica e ao Broker, enquanto que a Catalogação de Vulnerabilidades e Exploits será feita ao Broker.

1.2 Objetivos

Este relatório tem como propósito principal a identificação e descrição das ameaças de segurança presentes na infraestrutura, utilizando o modelo STRIDE como referência para a Modelação das Ameaças. Além disso, pretende-se analisar o impacto e a facilidade de exploração de cada ameaça identificada, classificando-as em níveis de risco. Com base nessas análises, serão propostas medidas de mitigação para cada ameaça, visando fortalecer a segurança e proteger os sistemas contra possíveis ataques. Por fim, procura-se contribuir para a melhoria contínua da segurança da informação no contexto do sistema de saúde, promovendo a autenticidade, confidencialidade, integridade e disponibilidade dos dados médicos e pessoais dos pacientes.

2 Metodologia Implementada

Nesta secção, irá ser explicada a estrutura do relatório, detalhando as estratégias escolhidas para identificar e descrever potenciais problemas de segurança que o sistema de suporte à interoperabilidade segura de dados médicos poderá ter. As diferentes secções correspondem à Modelação de Ameaças, onde vamos modelar as ameaças focando no Software através do uso da metodologia STRIDE apresentada nos slides das aulas e à Catalogação das Vulnerabilidades e Exploits para as Entidades cujas ferramentes já se encontram implementadas ou para as quais já se sabe quais as ferramentas/frameworks que vão ser utilizadas.

2.1 Modelação de Ameaças

Para a modelação de ameaças, são sugeridas as seguintes categorias:

- Focada nos Ativos - Este tipo de modelagem de ameaças concentra-se nos ativos críticos de um sistema, como dados confidenciais, propriedade intelectual, infraestrutura de rede, sistemas de controle industrial, entre outros. Identificar as ameaças específicas que podem visar esses ativos permite que as organizações foquem os seus esforços de segurança e aloquem recursos de maneira eficiente para proteger o que é mais importante para as mesmas.
- Focada nos Atacantes - Neste tipo de modelação, o foco está nos diferentes perfis e motivações dos atacantes que podem visar um sistema. Isso pode incluir ameaças como hackers individuais, grupos de hackers, agentes de ameaças persistentes avançadas, criminosos cibernéticos, entre outros. Compreender as táticas, técnicas e procedimentos dos atacantes é essencial para desenvolver estratégias eficazes de defesa cibernética.
- Focada no Software - Modelação de ameaças concentra-se nas vulnerabilidades e falhas de segurança no próprio software. Isto inclui ameaças como exploits de software, malware, backdoors e outras técnicas que visam explorar fraquezas nas aplicações ou sistemas de software.

Para a realização da modelação deste trabalho, foi escolhida a modelação focada no software, utilizando o modelo STRIDE que é amplamente utilizado para identificar e categorizar seis tipos comuns de ameaças que podem afetar um sistema de software. O acrônimo STRIDE representa os seguintes tipos de ameaças:

- Spoofing of Identity (Falsificação de Identidade): Esta ameaça ocorre quando alguém ou algo se faz passar por outra entidade legítima, enganando o sistema para obter acesso não autorizado. Exemplos incluem falsificação de endereço IP, usurpação de identidade de utilizador e falsificação de certificados digitais.

- Tampering with Data (Manipulação de Dados): Nesta ameaça, os dados são alterados de forma não autorizada, comprometendo a sua integridade. Isto pode resultar na apresentação de informações falsas ou na realização de cálculos incorretos. Exemplos incluem a alteração de dados em trânsito, adulteração de ficheiros e modificação de parâmetros de URL.

- Repudiation (Repúdio): Este tipo de ameaça permite que um utilizador negue ter realizado uma ação ou transação. Isto pode acontecer quando não existem registos adequados ou controlos de auditoria para rastrear as ações dos utilizadores. Exemplos incluem a negação de participação numa transação financeira ou a negação de envio de uma mensagem de correio eletrónico.

- Information Disclosure (Divulgação de Informações): Nesta ameaça, informações sensíveis são reveladas a indivíduos não autorizados. Isto pode resultar em violações de privacidade ou divulgação de segredos comerciais. Exemplos incluem a fuga de dados pessoais, exposição de informações confidenciais em registos de erro e exibição de mensagens de erro detalhadas que revelam informações sensíveis.

- Denial of Service (Negação de Serviço): Nesta categoria, o objetivo é sobrecarregar ou incapacitar um sistema, tornando-o inacessível aos utilizadores legítimos. Isto pode ser feito através de ataques de negação de serviço distribuídos (DDoS), exploração de vulnerabilidades de software ou esgotamento de recursos do sistema.

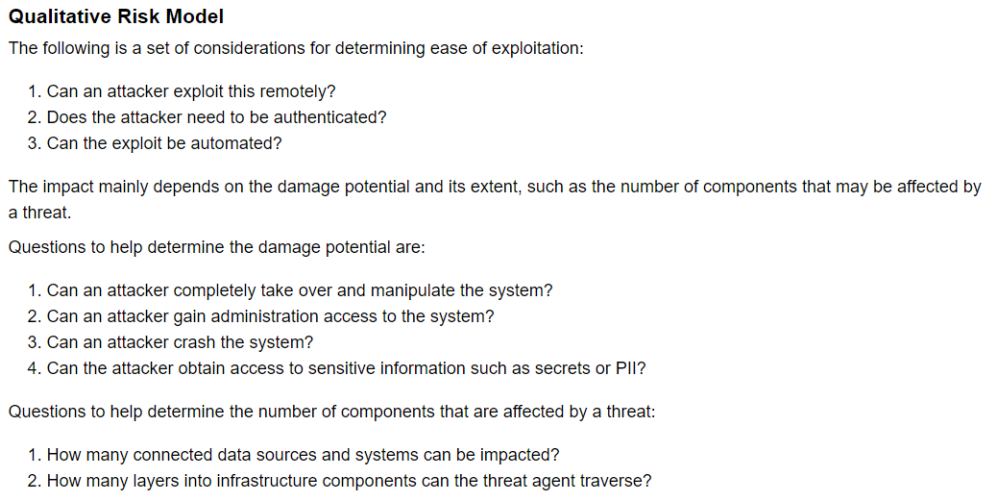
- Elevation of Privilege (Elevação de Privilégio): Esta ameaça ocorre quando um utilizador obtém acesso a recursos ou funcionalidades para os quais não deveria ter permissão. Isto pode permitir que o utilizador execute ações para além das suas autorizações normais, comprometendo a segurança do sistema. Exemplos incluem escalonamento de privilégios em sistemas operativos, exploração de vulnerabilidades de segurança para obter acesso administrativo e acesso não autorizado a contas de utilizador privilegiadas.

De acordo com estas categorias, serão analisadas e categorizadas as ameaças que poderão fazer parte do sistema em causa, assim como uma análise de risco de cada uma das ameaças. Esta análise de risco será dividida nas seguintes categorias, de acordo com o "Threat Modeling Process"fornecido pelo OWASP:

- Impacto - Definido pelo potencial de dano e pelo número de componentes que serão afetados. Quanto maior o valor do impacto, maior o risco.

- Facilidade de Exploração - Incluí a facilidade de descoberta por parte de atacantes, facilidade de exploração das vulnerabilidades e a facilidade de reprodução dos ataques. Quanto maior, maior o risco.

Para ajudar na avaliação do risco das categorias referentes ao Impacto e à Facilidade de Exploração, serão colocadas as seguintes questões para cada uma:



Qualitative Risk Model

The following is a set of considerations for determining ease of exploitation:

1. Can an attacker exploit this remotely?
2. Does the attacker need to be authenticated?
3. Can the exploit be automated?

The impact mainly depends on the damage potential and its extent, such as the number of components that may be affected by a threat.

Questions to help determine the damage potential are:

1. Can an attacker completely take over and manipulate the system?
2. Can an attacker gain administration access to the system?
3. Can an attacker crash the system?
4. Can the attacker obtain access to sensitive information such as secrets or PII?

Questions to help determine the number of components that are affected by a threat:

1. How many connected data sources and systems can be impacted?
2. How many layers into infrastructure components can the threat agent traverse?

Figura 2.1: Considerações para classificação das categorias na análise de risco

Todas estas categorias de risco irão ser classificadas segundo valores qualitativos, tais como Baixo, Médio, Alto ou combinações dos mesmos, de modo a reduzir a subjetividade que seria introduzida na avaliação caso fossem usados valores numéricos como noutros modelos de modelação de ameaças. É importante mencionar que o parâmetro "Possibility"é deixado de fora desta análise, uma vez que irão ser apresentadas formas de mitigação para que no momento da sua implementação, estas ameaças sejam totalmente mitigadas.

O objetivo é simplesmente avaliar o possível risco destas ameaças sem qualquer tipo de mitigação, de maneira a que a classificação do risco obtida seja o que irá determinar a lista de prioridades com as ameaças a mitigar, em que ameaças com maior risco deverão ser mitigadas primeiro.

2.2 Catalogação de Vulnerabilidades e Exploits

Nesta secção, irá ser feita a identificação e catalogação de vulnerabilidades e exploits existentes nas ferramentas que a infraestrutura vai usar, seja para as Entidadades que já se encontram implementadas, como para aquelas que ainda não estão implementadas mas em que se sabe quais as ferramentas que as mesmas vão utilizar.

Tendo em conta o objetivo deste trabalho, no caso de existirem várias vulnerabilidades para uma ferramenta em específico, o ideal será efetuar uma pesquisa de vulnerabilidades que causem um alto impacto no sistema em questão e em que o seu elevado risco possa pôr em causa a segurança da infraestrutura. Para avaliar este risco, será utilizado o CVSS Score (Common Vulnerability Scoring System Score), em que quanto maior o seu valor, maior é o risco que a vulnerabilidade apresenta, uma vez que este é um valor numérico atribuído a cada vulnerabilidade com base na sua gravidade, impacto e

potencial de exploração. Como fator de desempate será usado o EPSS (Exploit Prediction Scoring System Score) cuja pontuação indica a probabilidade de uma vulnerabilidade ser explorada. Este sistema atribui uma pontuação a cada vulnerabilidade com base numa variedade de fatores, incluindo a complexidade do exploit, a disponibilidade de ferramentas de exploração, a visibilidade da vulnerabilidade e a probabilidade de o exploit ser usado com sucesso.

Finalmente, para cada um dos softwares, será feita uma breve análise crítica sobre a escolha da versão desse software, se esta deverá ser trocada/atualizada ou se estará dentro dos parâmentros de segurança desejados.

3 Modelação de Ameaças - STRIDE

Antes de dar início ao processo de Modelação de Ameaças, é preciso entender quais são as Entidades que pertencem diretamente ao sistema e quais é que são as Entidades externas com as quais o Sistema interage. Esta distinção é importante porque esta modelação de ameaças será feita apenas para Entidades internas à Infraestrutura, tendo no entanto em conta as interações que existirão entre as mesmas e as Entidades Externas mencionadas, tais como as Bases de Dados das Unidades de Saúde e a Autoridade Certificadora.

Posto isto, a Modelação de Ameaças será feita para as seguintes Entidades:

- Aplicação do Paciente
- Aplicação Médica
- Broker

3.1 Aplicação do Paciente

A Aplicação do Paciente é uma aplicação móvel disponível para sistemas Android e iOS, destinada a armazenar e gerir os dados pessoais e de identificação do utilizador, juntamente com o seu certificado digital. Durante o processo inicial de utilização, estabelece uma ligação com a Autoridade Certificadora para descarregar os dados e o Certificado Digital do Paciente, garantindo segurança e integridade. Utiliza um QR Code para iniciar a comunicação com a Aplicação Médica, suportada por tecnologias como BLE, NFC ou WiFi-Aware.

A comunicação entre as aplicações é assegurada por mensagens codificadas em JSON, garantindo confidencialidade e integridade dos dados. Durante uma consulta médica, o profissional utiliza a Aplicação Médica para estabelecer um canal seguro com a Aplicação do Paciente, onde o paciente pode autorizar o acesso aos seus dados, enviando um token de autorização e o seu Certificado Digital.

De seguida, vamos dar entãi inicio à Modelação de Ameaças para a Aplicação do Paciente.

3.1.1 Spoofing - Authentication

1 - Credenciais do paciente armazenadas de forma insegura

Uma das ameaças associadas aos ataques de spoofing ocorre quando uma entidade maliciosa obtém as credenciais de autenticação do utilizador da aplicação, as quais estão armazenadas no sistema sem estarem cifradas. Isto pode acontecer se a senha for

armazenada em texto simples ou se for facilmente identificada através da descoberta de padrões entre as senhas armazenadas. Desta forma, o atacante pode aceder à conta do paciente, permitindo-lhe realizar operações e funcionalidades em nome do mesmo.

Mitigação da Ameaça

Como forma de mitigação desta ameaça, é necessária a implementação de mecanismos que cifram as credenciais de forma segura, utilizando algoritmos de PBKDFs, que derivam um hash de uma password, utilizando uma função pseudo-aleatória, sendo esse o hash armazenado no sistema. O uso de funções de HASH simples é desaconcelhado uma vez que deixam o sistema alvo de ataques de dicionário em que um atacante consegue descibrir padrões entre as passwords utilizadas pelo utilizador comum e a as passwords que os pacientes na nossa aplicação poderão ter escolhido.

O uso de PBKDFs, que a partir da password e de salt pseudo-aleatório derivam um hash sempre diferente, mesmo para passwords iguais, faz com que seja necessário ter acesso ao valor do salt, aumentando assim a segurança. Isto diminui drasticamente o risco de um atacante ter sucesso na obtenção das credenciais de um paciente e consequentemente obter acesso à sua conta, o que lhe permitiria ter acesso a todas as funcionalidades e dados confidenciais da mesma.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Alta
- Risco Final - Alto

Esta ameaça terá sem dúvida um impacto alto no sistema, uma vez que um atacante que consiga obter as credenciais de acesso de um paciente, terá imediatamente acesso a informações confidenciais do mesmo e a funcionalidades da aplicação do paciente. No entanto, está explicíto nos requisitos a existência de mecanismos robustos de autenticação e confidencialidade de dados, pelo que esta será uma ameaça facilmente mitigada com o uso dos algoritmos mencionados na secção de mitigação.

Com isto, o risco final atribuído a esta ameaça é de Alto, uma vez que esta ameaça poderá pôr em causa a aplicação dos pacientes, diminuindo a confiabilidade por parte dos mesmos em todo o sistema, assim como expôr informações e funcionalidades críticas.

2 - Ausência de Autenticação Forte

Um dos riscos relacionados aos ataques de spoofing surge quando uma entidade maliciosa consegue adquirir as credenciais de autenticação do utilizador da aplicação, devido à sua vulnerabilidade e facilidade de obtenção, o que ocorre principalmente quando a senha é fraca. Como resultado, a entidade maliciosa pode ter acesso à conta do paciente, possibilitando-lhe realizar ações e operações em nome do mesmo. Esta ameaça vai de encontro à última ameaça uma vez que os resultados finais da exploração da ameaça

são os mesmos, apenas se altera a razão pela qual a mesma acontece e os seus métodos de exploração.

Mitigação da Ameaça

Como métodos de mitigação para esta ameaça, será necessário implementar dois aspetos no sistema para a autenticação do paciente. O primeiro está relacionado com a existência da obrigação de uma password forte por parte do paciente, diminuindo a probabilidade de que esta seja encontrada por uma atacante em por exemplo ataques de brute-forcing. O segundo prende-se com a implementação de um sistema de Autenticação Multi-Fator, introduzindo uma camada extra de segurança, fazendo com que mesmo que um atacante obtenha as credenciais da conta de um ou vários pacientes, este não consiga obter acesso às contas e consequentemente a dados confidenciais ou funcionalidades referentes aos pacientes.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Alta
- Risco Final - Alto

Se forem aplicados os métodos de mitigação mencionados, a possibilidade de exploração desta ameaça será reduzida drasticamente. No entanto, o impacto e facilidade de exploração são bastante altos, pelas mesmas razões verificadas na última ameaça. Posto isto, é atribuído um risco Alto a esta ameaça que terá as mesmas consequências da última ameaça.

3 - Falsificação de dados na Autenticação

Uma das ameaças associadas a ataques de Spoofing diz respeito à falsificação de dados enviados por atacantes, fazendo com que os pacientes pensem que os dados são enviados por entidades de confiança. Isto poderá permitir o envio de informações sensíveis por parte dos pacientes, uma vez que estes não têm noção de que efetuaram uma comunicação com uma entidade maliciosa em vez da entidade do sistema a que se pretendiam conectar.

Mitigação da Ameaça

Como mitigação desta ameaça, deverão ser implementados mecanismos seguros de autenticação e verificação nos momentos em que são gerados parãmetros de conexão, tais como endereços IP ou ID's de conexão BLE e NFC. Estes mecanismos passam pela implementação do uso de passwords ou assinaturas digitais para a existência de uma autenticação forte.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Alta
- Risco Final - Alto

A análise de risco desta ameaça vai de encontro às outras duas ameaças que vimos.

3.1.2 Tampering - Integrity

1 - Falta de autenticação entre Entidades para transferências de dados

Esta ameaça diz respeito à falta de autenticação entre Entidades, dando oportunidade a atacantes para modificarem as mensagens enviadas entre as mesmas. Uma vez que são usados canais TCP/IP para a comunicação entre por exemplo a Autoridade Certificadora e a Aplicação do Paciente, é possível que um atacante intercete e modifique as mensagens enviadas nestes canais, tais como os dados do Paciente ou o Certificado Digital, fazendo uso da falta de autenticação nos dados enviados.

Mitigação da Ameaça

Como mitigação para esta ameaça, poderá ser utilizado um algoritmo de hashing tal como o SHA-256, que cria um hash a ser enviado em conjunto com os dados a serem transferidos. Na Aplicação do Paciente, este irá fazer a verificação do hash recebido e do hash da mensagem recebida. Se estes forem iguais, a mensagem não terá sido adulterada e os dados serão aceites.

Análise de Risco

- Impacto - Baixo-Médio
- Facilidade de Exploração - Alta
- Risco Final - Médio

Esta é uma ameaça que podemos considerar de fácil exploração, não sendo no entanto crítica a ponto de ter um impacto alto, uma vez que a adulteração dos dados transferidos tem interferência apenas na integridade e confidencialidade dos dados, não afetando especificamente o sistema no seu todo. É atribuído um risco final de Médio.

2 - Logs armazenados na Aplicação do Paciente

Esta ameaça diz respeito à armazenação dos logs das interações entre um Paciente e um Médico, mais especificamente no armazenamento dos logs dessas interações nos dispostivos dos Pacientes, o que poderá pôr em causa a integridade dos dados para auditorias posteriores, uma vez que estes dados podem ser perdidos ou adulterados.

Mitigação da Ameaça

Para mitigação desta ameaça, os logs deverão ser armazenados numa Entidade externa, sendo esta por exemplo o Broker, de maneira a que os logs sejam mantidos de forma segura e que uma posterior auditoria possa ser efetuada sem o risco de existir falta de dados ou de dados adulterados. Uma opção seria o envio de logs por parte da Aplicação Médica para o Broker, assim que esta recebe o token de autorização e o certificado digital do Paciente, bem como o envio de logs assim que a Unidade de Saúde referente ao Médico que se conectou ao Paciente receba os atributos do Paciente de outras Unidades de Saúde.

Análise de Risco

- Impacto - Baixo
- Facilidade de Exploração - Média
- Risco Final - Baixo-Médio

Esta é uma ameaça com um risco final considerado de Baixo-Médio, uma vez que não afeta diretamente o funcionamento do sistema, sendo apenas uma funcionalidade adicional a ser adicionada ao sistema para aumentar a integridade e consistência dos dados de todo o sistema.

3 - Alteração e Armazenamento de Dados alterados do Paciente

Esta ameaça pode ser caracterizada por duas fases e diz respeito à possibilidade de alteração dos dados guardados no dispositivo do Paciente, bem como o armazenamento desses mesmos dados alterados numa fase posterior por outras Entidades. Na primeira, um atacante ou até mesmo o próprio paciente pode de alguma maneira alterar os dados se não forem tidos os devidos cuidados, sendo que numa segunda fase, estes mesmos dados alterados podem ser enviados para as outras Entidades tal como a Aplicação Médica, pondo em causa a integridade dos dados em circulação.

Mitigação da Ameaça

Como mitigação para esta ameaça, será necessário que os dados armazenados no dispositivo do Paciente se encontrem com permissões que não lhe permitam, ou a um atacante, alterar os mesmos, nomeadamente permissões de leitura, sendo que apenas a Aplicação do Paciente deverá ter permissões de escrita para que possa alterar os dados sempre que houver uma atualização por parte dos dados enviados pela Autoridade Certificadora.

Em relação ao armazenamento destes dados modificados, a solução será a utilização de algoritmos que permitam a assinatura digital destes mesmos dados, na fase em que são enviados pela Autoridade Certificadora, de maneira a que no momento em que a Aplicação Médica recebe os dados do Paciente para enviar para o Broker, seja possível fazer a verificação dos dados e saber se houve alguma alteração maliciosa nos mesmos.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Baixa
- Risco Final - Médio

Esta é uma ameaça que põe em causa a integridade e autenticidade dos dados no sistema, sendo no entanto de difícil acesso por parte de atacantes, uma vez que teriam que ganhar acesso ao dispositivo do Paciente. No entanto, poderá ter algum impacto uma vez que todo o sistema funciona com base nos dados do Paciente, não havendo no entanto perigo de que o sistema fosse comprometido pela alteração dos mesmos. O risco final atribuído é de Médio.

3.1.3 Repudiation - Non-Repudiation

1- Envio de dados não assinados entre Aplicação do Paciente e outras Entidades

A principal ameaça associada ao envio de dados não assinados entre Entidades é o potencial de repúdio, onde por exemplo a Aplicação do Paciente não consegue rastrear atividades maliciosas enviadas a partir da mesma ou de outras Entidades para ela. Isto torna impossível para as Entidades identificarem se quem realizou o envio de dados foram de facto as Entidades em questão ou se foram Entidades maliciosas. Um atacante poderia enviar dados maliciosos a partir da Aplicação do Paciente para as já referidas Entidades, sem que essas entidades percebam que os dados foram enviados por uma entidade malicios ou o contrário.

Mitigação da Ameaça

Para mitigar esta ameaça, é essencial implementar a autenticação mútua entre a Aplicação do Paciente e as restantes Entidades com quem este comunica. Isto pode ser alcançado através do uso de certificados digitais para autenticar tanto o Paciente quanto as outras Entidades. Com a autenticação mútua, tanto o Paciente quanto as Entidades podem confirmar a identidade uns dos outros antes de iniciar a transferência de dados. Além disso, é crucial que os dados sejam assinados digitalmente para garantir sua autenticidade e integridade durante a transferência.

Análise de Risco

- Impacto - Médio
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

Dado que o envio de dados não assinados entre a Aplicação do Paciente e outras Entidades pode resultar em repúdio, o impacto dessa vulnerabilidade pode ser considerado médio, uma vez que embora a negação da origem dos dados possa criar confusão e dificultar a identificação do responsável, os danos diretos podem não ser imediatamente significativos. No entanto, a longo prazo, essa falta de autenticação e não-repúdio pode comprometer a integridade do sistema e a confiança nas transações.

Quanto à facilidade de exploração, pode ser classificada como média a alta. A exploração dessa vulnerabilidade requer conhecimento técnico para manipular os dados enviados pela Aplicação do Paciente sem a devida assinatura. No entanto, se um atacante conseguir aceder e comprometer a Aplicação do Paciente, eleeste pode facilmente enviar dados não assinados, aproveitando-se da ausência de mecanismos de autenticação adequados.

3.1.4 Information Disclosure - Confidentiality

1 - Armazenamento de Dados do Paciente na Aplicação

Para a Information Disclosure, no que diz respeito à confidencialidade dos dados do Paciente, a primeira ameaça diz respeito aos dados do Paciente que são armazenados na Aplicação do Paciente e que poderão estar vulneráveis a atacantes que pretendem obter acesso aos mesmos, de modo a obterem informações confidenciais sobre os Pacientes.

Mitigação da Ameaça

É fundamental adotar uma abordagem que aborde as várias frentes desta ameaças. Primeiramente, todos os dados pessoais armazenados na aplicação do paciente devem ser criptografados. Esta medida garante que, mesmo que um atacante consiga aceder os dados, eles permaneçam ilegíveis sem a chave de descriptografia correspondente. Além disso, implementar controlos de acesso robustos é crucial. Isto envolve a utilização de autenticação forte, como senhas robustas, autenticação de dois fatores ou biometria, para garantir que apenas usuários autorizados tenham acesso aos dados. Por fim, minimizar a coleta de dados é uma estratégia eficaz para reduzir o risco. Coletar apenas os dados pessoais estritamente necessários diminui o volume de dados sensíveis armazenados e, consequentemente, o potencial de exposição em caso de violação.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média
- Risco Final - Médio-Alto

O impacto do vazamento de dados pessoais e confidenciais poderá ser considerado alto uma vez que estes serão dados sensíveis, podendo levar até a repercussões legais e financeiras para a nossa organização. No que diz respeito à facilidade de exploração da

mesma, podemos considerar que é Médio, dependendo sempre das medidas de segurança globais implementadas na Aplicação, exigindo de qualquer das maneiras um elevado grau de habilidade técnica para proceder á exploração desta ameaça.

2 - Armazenamento de Certificados Digitais do Paciente na Aplicação

Para a Information Disclosure, no que diz respeito à confidencialidade dos dados do Paciente, a primeira ameaça diz respeito aos certificados digitais que são armazenados na Aplicação do Paciente e que poderão estar vulneráveis a atacantes que pretendem obter acesso aos mesmos, de modo a usarem esses Certificados Digitais para explorar outras ameaças

Mitigação da Ameaça

Como formas de mitigação, deverão ser implementados mecanismos de criptografia de dados para os certificados digitais usando algoritmos robustos, bem como o armazenamento seguro dos mesmos usando mecanismos como o Android Keystore ou o iOS Keychain para a judar a proteger os certificados contra acessos não autorizados. Para além disto, deverão ser implementados controlos de acesso rigorosos de maneira a que apenas a Aplicação do Paciente tenha permissões para modificar os dados do mesmo.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Média-Baixa
- Risco Final - Médio

O impacto do vazamento de Certificados Digitais poderá ser considerado médio-alto em que se os certificados digitais forem utilizados para autenticação e autorização no sistema, a sua exposição pode comprometer a integridade e a confidencialidade das comunicações, bem como abrir caminho para ataques de falsificação de identidade ou de phishing mais sofisticados.. No que diz respeito à facilidade de exploração da mesma, podemos considerar que é média-baixa, uma vez que será algo desafiante de explorar para um atacante, especialmente com a implementação das medidas de segurança adequadas.

3.1.5 Denial of Service - Availability

Ataques de Negação de Serviço - Aplicação do Paciente

Os ataques de negação de serviço têm como objetivo tornar os recursos de um sistema inacessíveis para os seus utilizadores. Geralmente, os alvos desses ataques são servidores, uma vez que é crucial que estejam sempre disponíveis para que os utilizadores possam aceder às informações contidas neles. No caso da aplicação do paciente, estes ataques não seriam preocupantes, uma vez que as aplicações geralmente não são alvo desse tipo

de ataque, já que não é necessário que estejam sempre disponíveis para a obtenção de informações.

Estes ataques são normalmente direcionados para entidades como o Broker ou a Autoridade Certificadora, pois é fundamental que estejam sempre disponíveis para responder aos pedidos e comunicar com as outras entidades do sistema. Portanto, esses ataques não são aplicados à entidade em questão. Mais á frente iremos ver para Entidade Broker quais as ameaças a que este estará exposto para as ameaças de DoS.

3.1.6 Elevation of Privilege - Authorization

1 - Obtenção de acesso a recursos e funcionalidades da Aplicação do Paciente

Esta ameaça refere-se à possibilidade de um atacante obter acesso a recursos ou funcionalidades da aplicação que normalmente não teria permissão para acedar. Isto pode incluir a capacidade de realizar ações privilegiadas, como aceder dados confidenciais dos pacientes ou até mesmo modificar dados ou certificados digitais.

Um atacante poderia usar este acesso priveligiado para alterar as permissões relacionadas com os ficheiros dos dados ou dos certificados digitais na Aplicação do Paciente de maneira a conseguir modificar os mesmos.

Mitigação da Ameaça

Como forma de mitigação, seria necessária a implementação de mecanismos de autenticação forte, tal como visto nas ameaças anteriores, assim como proteger os dados armazenados na Aplicação do Paciente com técnincas de criptografia, garantindo que mesmo que um atacante se conseguisse autenticar, os dados permaneceriam ilegíveis e inutilizáveis.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

Esta ameaça pode resultar em acessos não autorizados a informações confidenciais dos pacientes, comprometendo a sua privacidade e integridade dos dados, levando a que o impacto considerado seja Alto. Em termos da facilidade de exploração, esta é considerada Médio-Alto, sendo no entanto a sua exploração bastante mais dificil caso sejam implementadas as medidas de mitigação mencionadas

3.2 Aplicação Médica

Tal como a aplicação do paciente, a aplicação médica também é uma aplicação móvel para dispositivos que operam com os sistemas Android e iOS, ou qualquer outro

dispositivo compatível com os protocolos de comunicação e operações mencionados anteriormente. Através desta aplicação, um profissional de saúde estabelece contacto com o paciente e solicita os atributos necessários para o tratamento específico.

Embora seja esta aplicação que controla o processo de solicitação de atributos, é importante destacar que os dados do paciente não devem ser armazenados no dispositivo em uso. Pelo contrário, os dados fornecidos por uma unidade de saúde devem ser armazenados na respetiva base de dados, na qual o profissional de saúde está a fornecer assistência ao paciente. Assim sendo, é crucial que o pedido enviado pela aplicação médica ao broker inclua os mecanismos necessários para associá-lo à unidade de saúde à qual os dados serão enviados.

É importante mencionar que nesta secção de Modelação de Ameaças da Aplicação Médica, a maior parte das ameaças já foram referidas na Aplicação do Paciente, uma vez que as mesmas envolviam na maior parte das vezes a Aplicação Médica, sendo esta a Entidade principal com quem a Aplicação do Paciente interage.

Posto isto, e tal como foi feito para a Aplicação do Paciente, vamos aplicar o modelo STRIDE para esta Entidade.

3.2.1 Spoofing - Authentication

Autenticação

Para esta secção do Spoofing, é possível modelar as ameaças de acordo com as ameaças vistas na Aplicação do Paciente, nomeadamente, fazendo apenas a alteração para os utilizadores da Aplicação Médica, nomeadamente os profissionais de saúde:

- Credenciais dos profissionais de saúde armazenadas de forma insegura.
- Ausência de Autenticação Forte.
- Falsificação de dados na Autenticação.

Mitigação da Ameaça

Em termos de mitigação, as técnicas a implementar são as mesmas que aquelas que vimos para a Aplicação do Paciente, com uma nota importante para a ausência de Certificado Digital na descrição do Sistema. De maneira a garantir métodos robustos de autenticação e de integridade dos dados enviados entre Entidades, será vital para o sistema que também a Aplicação do Paciente comunique com a Autoridade Certificadora de maneira a obter e manter atualizado o seu Certificado Digital, para que este possa ser enviado nos momentos em que os pedidos entre as mesmas Entidades são feitos.

Esta será uma medida de mitigação que ajudará nas ameaças das próximas secções, tal como vimos na Aplicação do Paciente.

Análise de Risco

- Impacto - Alto

- Facilidade de Exploração - Alta
- Risco Final - Alto

Em termos de risco destas ameaças para o sistema, será possível dizer que o risco de Entidades maliciosas acederem à Aplicação Médica será maior do que na Aplicação do Paciente. Isto acontece porque esta comunica com todas as Entidades do Sistema e tem por sua vez acesso a todos os dados que estariam em causa nas ameaças vistas na secção da Aplicação do Paciente.

A Aplicação Médica tem acesso a todos os dados médicos do Paciente, assim como o Certificado Digital do mesmo que lhe é enviado no inicio da interação entre Paciente e Profissional de Saúde para que seja dado inicio ao processo de obtenção dos dados médicos do Paciente.

Por outro lado, a Aplicação Médica também comunica com a Autoridade Certificadora de maneira a obter o seu próprio Ceritificado Digital e com as Unidades de Saúde que lhe transmitem os dados dos Pacientes.

Tendo em conta todos estes aspetos, é possível dizer que todas estas ameaças são considerados de risco Alto.

3.2.2 Tampering - Integrity

1 - Interceção e alteração de pedidos da lista de atributos médicos

Um atacante pode tentar interceptar os pedidos enviados pela Aplicação Médica para a Aplicação do Paciente e alterar os atributos médicos solicitados. Isto pode resultar na obtenção de informações médicas incorretas ou na inclusão de informações falsas nos pedidos.

Mitigação da Ameaça

Um método eficaz para mitigar esta ameaça é a implementação de criptografia de ponta a ponta nas comunicações entre a Aplicação Médica e a Aplicação do Paciente. Isto garantirá que o pedido para obtenção da lista de atributos médicos seja protegido durante a transmissão, impedindo que um atacante o intercepte e o altere. Além disso, o uso de assinaturas digitais nos pedidos enviados pela Aplicação Médica pode ajudar a garantir a integridade dos dados, permitindo que a Aplicação do Paciente valide a origem dos pedidos.

Análise de Risco

- Impacto - Médio
- Facilidade de Exploração - Média
- Risco Final - Médio

Esta ameaça apresenta um impacto médio, uma vez que a interceção e alteração dos pedidos da lista de atributos médicos podem resultar na divulgação de informações médicas sensíveis do paciente, comprometendo sua privacidade e segurança. Quanto à facilidade de exploração, é considerada média, pois embora a interceção dos pedidos possa exigir um certo nível de habilidade técnica, existem ferramentas disponíveis que podem facilitar a captura e modificação de comunicações não criptografadas.

2 - Falsificação de token de autorização e certificado digital

Um atacante pode tentar falsificar o token de autorização e o certificado digital enviados pela Aplicação do Paciente para a Aplicação Médica. Isto pode permitir que o atacante ganhe acesso não autorizado aos dados médicos do paciente ou que envie dados falsificados para a Aplicação Médica.

Mitigação da Ameaça

Uma abordagem eficaz para mitigar essa ameaça é implementar autenticação multifator para verificar a identidade do Profissional de Saúde antes de conceder acesso à Aplicação Médica, tal como visto na secção da Aplicação do Paciente. Isto pode envolver o uso de biometria ou tokens de segurança adicionais para garantir que apenas o Profissional de Saúde em questão tenha acesso aos dados médicos do Paciente. Além disso, é essencial validar cuidadosamente os certificados digitais apresentados pela Aplicação do Paciente para garantir sua autenticidade e integridade.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Baixa
- Risco Final - Médio

No que diz respeito à análise de risco, esta apresenta um impacto alto, uma vez que a falsificação bem-sucedida do token de autorização e do certificado digital pode permitir que um atacante aceda a informações médicas confidenciais do paciente, comprometendo a sua privacidade e integridade a dos seus dados. Quanto à facilidade de exploração, é considerada baixa, pois a falsificação destes tokens e certificados geralmente requer um conhecimento avançado em criptografia e manipulação de certificados digitais.

3 - Modificação de pedidos enviados para o Broker

Um atacante pode tentar modificar os pedidos enviados pela Aplicação Médica para o Broker, alterando o token de autorização, os certificados digitais e os dados da Unidade de Saúde. Isto pode resultar na obtenção de acesso não autorizado aos dados do paciente ou na manipulação dos dados durante a transferência.

Mitigação da Ameaça

Para mitigar esta ameaça, é fundamental incluir assinaturas digitais nos pedidos enviados pela Aplicação Médica para o Broker. Essas assinaturas garantirão a integridade e autenticidade dos dados, permitindo que o Broker valide a origem e integridade dos pedidos recebidos. Além disso, a implementação de controlos de acesso baseados em funções (RBAC) pode ajudar a restringir as ações que a Aplicação Médica pode realizar no Broker, reduzindo assim o risco de manipulação de dados por utilizadores não autorizados.

Análise de Risco

- Impacto - Médio
- Facilidade de Exploração - Média
- Risco Final - Médio

A ameaça em causa apresenta um impacto médio, uma vez que a modificação de pedidos enviados para o Broker pode resultar na divulgação de informações médicas sensíveis ou na execução de ações não autorizadas, comprometendo a integridade e segurança dos dados do paciente. Quanto à facilidade de exploração, é considerada média, pois a modificação de pedidos pode exigir acesso aos sistemas ou comunicações entre a Aplicação Médica e o Broker, o que pode ser alcançado por meio de técnicas de ataque como interceção de tráfego ou exploração de vulnerabilidades de software.

4 - Interceção e modificação dos dados durante a transferência entre unidades de saúde

Um atacante pode tentar interceptar e modificar os dados durante a transferência entre as unidades de saúde. Isto pode resultar na adulteração dos dados médicos do paciente ou na inclusão de informações falsas nos dados transferidos.

Mitigação da Ameaça

Para mitigar esta ameaça, é essencial utilizar criptografia robusta durante a transferência de dados entre as unidades de saúde. Protocolos como TLS/SSL podem garantir a segurança das comunicações, protegendo os dados contra interceção e alteração por parte de terceiros. Além disso, é importante implementar mecanismos de verificação de integridade dos dados durante a transferência, como hashes ou checksums, para garantir que os dados recebidos não tenham sido modificados durante a transmissão.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Baixo

- Risco Final - Médio

Esta ameaça apresenta um impacto alto, uma vez que a interceção e modificação de dados durante a transferência entre unidades de saúde podem resultar na divulgação ou corrupção de informações médicas sensíveis do paciente, comprometendo a sua privacidade, integridade e disponibilidade. Quanto à facilidade de exploração, é considerada baixa, pois embora a interceção de dados possa ser possível em redes desprotegidas, a modificação bem-sucedida dos dados geralmente requer acesso privilegiado aos sistemas envolvidos, tornando-a uma tarefa mais difícil para invasores externos.

3.2.3 Repudiation - Non-Repudiation

1 - Recusa de Autorização por Parte do Paciente

Esta ameaça refere-se à possibilidade de o paciente negar ter concedido autorização para acesso aos seus dados médicos, mesmo que o pedido tenha sido legítimo. Isso pode ocorrer devido a vários motivos, como esquecimento, má compreensão das solicitações de autorização ou mesmo negação deliberada após a autorização ter sido concedida.

Mitigação da Ameaça

Uma forma eficaz de mitigar essa ameaça é garantir que todas as interações entre o paciente e a aplicação sejam registadas de forma detalhada e imutável. Isto pode ser alcançado implementando um sistema de logs para uma auditoria posterior que registe todo o processo de solicitação de acesso por parte da Aplicação Médica à Aplicação do Paciente. Estes logs devem ser armazenados de forma segura e protegidos contra adulteração, de preferência no Broker.

Além disto, é importante implementar mecanismos de autenticação robustos, como autenticação de dois fatores, para garantir que apenas o paciente legítimo possa autorizar o acesso aos seus dados. Isto pode ajudar a reduzir a probabilidade de negação de autorização injustificada.

Análise de Risco

- Impacto - Médio
- Facilidade de Exploração - Baixa
- Risco Final - Médio-Baixo

Para esta ameaça, o impacto é considerado médio, uma vez que a recusa de autorização pode comprometer a integridade dos registos médicos e a confiabilidade das interações no sistema. A facilidade de exploração é baixa, pois exige que o paciente recuse ativamente a autorização, o que não é facilmente alcançado sem a sua intervenção direta. No entanto, é possível que fatores como erros de interface ou manipulação possam aumentar a probabilidade de recusa não intencional. O risco final atribuído é de médio-baixo.

2 - Manipulação de Registos de Interacções

Esta ameaça refere-se à possibilidade de um atacante manipular ou falsificar os registos de interações entre a Aplicação do Paciente e a Aplicação Médica para ocultar atividades maliciosas. Os atacantes podem tentar modificar ou excluir logs de transações legítimas para encobrir as suas ações ou criar registos falsos para simular atividades legítimas que não ocorreram realmente.

Mitigação da Ameaça

Uma forma eficaz de mitigar esta ameaça é a de implementar mecanismos de auditoria e registo robustos que registem todas as interações entre a Aplicação do Paciente e a Aplicação Médica de forma imutável e transparente. Isto pode ser alcançado por meio de tecnologias como registoos distribuídos como a blockchain ou bases de dados com controlo de acesso rigoroso.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média
- Risco Final -

Para esta ameaça, o impacto é alto, uma vez que a manipulação dos registos pode levar a diagnósticos errados, tratamentos inadequados ou perda de confiança no sistema de saúde. A facilidade de exploração é considerada média, uma vez que pode envolver a manipulação de dados no sistema ou acesso não autorizado aos registos médicos, mas é mitigável com controlos adequados de acesso e monitorização de atividades suspeitas.

3.2.4 Information Disclosure - Confidentiality

1 - Revelação não autorizada de dados médicos do paciente

Nesta ameaça, existe o risco de que os dados médicos dos pacientes, uma vez solicitados pela aplicação médica, possam ser revelados a terceiros não autorizados durante a transmissão ou processamento. Isto pode ocorrer devido a falhas de segurança na comunicação entre a Aplicação Médica e a Aplicação do Paciente ou do Broker.

Mitigação da Ameaça

Para mitigar este risco, é fundamental implementar protocolos de segurança robustos para proteger a comunicação entre a Aplicação Médica, a Aplicação do Paciente e outros sistemas. Isto pode incluir o uso de criptografia forte para garantir a confidencialidade dos dados durante a transmissão. Além disso, é importante implementar controlos de acesso adequados para garantir que apenas utilizadores autorizados tenham permissão para aceder os dados médicos dos pacientes. A autenticação mútua também deve ser empregada para garantir a autenticidade das partes envolvidas na comunicação.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média
- Risco Final - Médio-Alto

O impacto desta ameaça pode ser considerado alto, uma vez que a divulgação não autorizada de dados médicos pessoais pode resultar em consequências graves para os pacientes, incluindo violação de privacidade, danos emocionais e até mesmo impactos negativos na saúde. Quanto à facilidade de exploração, esta ameaça pode ser classificada como média, pois requer conhecimento e habilidades técnicas para intercetar ou comprometer a comunicação entre os sistemas envolvidos. No entanto, a complexidade pode variar dependendo da eficácia das medidas de segurança implementadas.

2 - Revelação não autorizada de certificados digitais do paciente

Os certificados digitais do paciente, necessários para autenticação mútua durante as interações entre a Aplicação Médica e a Aplicação do Paciente, podem ser expostos a riscos de divulgação não autorizada. Isto pode acontecer se os certificados não forem devidamente protegidos durante a transmissão ou armazenamento, permitindo que terceiros maliciosos obtenham acesso não autorizado.

Mitigação da Ameaça

Uma medida eficaz para mitigar esta ameaça é a de garantir que os certificados digitais do paciente sejam protegidos durante a transmissão e armazenamento. Isto pode ser alcançado por meio do uso de técnicas de criptografia para proteger os certificados durante a transmissão entre a aplicação médica, a aplicação do paciente e outros sistemas. Além disso, é importante implementar controlos de acesso adequados para restringir o acesso aos certificados apenas a utilizadores autorizados.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Baixa
- Risco Final - Médio

O impacto desta ameaça também pode ser considerado alto, uma vez que a exposição dos certificados digitais do paciente pode comprometer a autenticidade e a integridade dos dados transmitidos, colocando em risco a confidencialidade das informações médicas. Em termos de facilidade de exploração, esta ameaça pode ser classificada como baixa, pois geralmente requer acesso privilegiado aos sistemas envolvidos ou técnicas sofisticadas de ataque para comprometer a segurança dos certificados digitais.

3 - Exposição de dados médicos durante o armazenamento na Aplicação Médica

Os dados médicos recebidos pela Aplicação Médica podem ser armazenados de forma inadequada, tornando-os vulneráveis a acessos não autorizados por parte de pessoal não autorizado ou até mesmo de atacantes externos. Isto pode resultar na divulgação não autorizada de informações sensíveis sobre os pacientes.

Mitigação da Ameaça

Para mitigar este risco, é essencial implementar medidas de segurança adequadas para proteger os dados médicos dos pacientes durante o armazenamento na aplicação médica. Isto pode incluir o uso de técnicas de criptografia para proteger os dados armazenados temporariamente, garantindo que apenas utilizadores autorizados tenham acesso aos dados armazenados. Além disto, é importante implementar controlos de acesso granulares para garantir que apenas pessoal autorizado tenha permissão para visualizar ou modificar os dados médicos dos pacientes. A realização regular de auditorias de segurança também pode ajudar a identificar e corrigir potenciais vulnerabilidades no armazenamento de dados.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

O impacto desta ameaça pode ser considerado alto, uma vez que a exposição de dados médicos sensíveis durante o armazenamento pode resultar em consequências semelhantes à revelação não autorizada durante a transmissão. Isto pode incluir a violação de privacidade, danos emocionais e impactos negativos na saúde dos pacientes. Quanto à facilidade de exploração, esta ameaça pode ser classificada como média a alta, pois o acesso não autorizado aos dados armazenados geralmente requer exploração de vulnerabilidades nos sistemas ou falhas nos controlos de acesso. O grau de dificuldade pode variar dependendo da eficácia das medidas de segurança implementadas e da sofisticação dos atacantes.

3.2.5 Denial of Service - Availability

Esta secção da negação de serviço para a aplicação médica encontra-se na mesma situação vista na aplicação do paciente, pelo que não faz grande sentido apresentar ameaças nesta secção.

É sempre possível que tanto a Aplicação do Paciente como a Aplicação Médica sejam alvo de ataques de negação serviço por exemplo em situações em que ambas as aplicações se conectam a outras Entidades ou estão à espera de receber informações das mesmas,

mas pelas características destas aplicações e pela maneira como a comunicação entre Entidades está construída, se as ameaças vistas até agora forem mitigadas, dificilmente haverá maneira de de efetuar ataques de negação de serviço que façam com a Aplicação de um Paciente ou de um Médico fiquem indisponíveis. Mesmo que estes aconteçam, o seu impacto para o sistema no global seria praticamente nulo.

3.2.6 Elevation of Privilege - Authorization

1 - Elevação de privilégios na Aplicação Médica

Esta ameaça refere-se à possibilidade de um atacante tentar obter acesso a recursos ou funcionalidades da aplicação médica para os quais não teria permissão normalmente. Se bem-sucedido, o atacante poderia explorar esses privilégios elevados para realizar atividades maliciosas, como aceder dados sensíveis dos pacientes, alterar registos médicos ou interromper o funcionamento normal da aplicação.

Mitigação da Ameaça

Como formas de mitigação, temos a implementação de um modelo de controlo de acesso robusto que limite os privilégios dos usuários com base nas suas funções e responsabilidades e que inclua a atribuição de permissões específicas apenas aos profissionais de saúde autorizados e a implementação de autenticação forte para verificar a identidade do utilizador tal como vimos na secção do Spoofing.

Por outro lado, a utilização de técnicas de criptografia para proteger os dados sensíveis armazenados na aplicação médica, garantindo que apenas utilizadores autorizados possam aceder aos mesmos. Isto pode ajudar a mitigar os riscos associados à elevação de privilégios, mesmo se um atacante conseguir acesso não autorizado à aplicação.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

A ameaça de elevação de privilégios na aplicação médica pode ter um impacto considerável, classificado como alto, uma vez que pode levar à exposição de dados sensíveis dos pacientes e comprometer a integridade e a confidencialidade das informações médicas. Em termos de facilidade de exploração, esta ameaça pode ser considerada média-alta, dependendo da eficácia das medidas de segurança implementadas e da habilidade do atacante em explorar vulnerabilidades no sistema. O risco final atribuído é de médio-alto

3.3 Broker

3.3.1 Spoofing - Authentication

1 - Falsificação de identidade na comunicação com o Broker

Nesta ameaça, um atacante pode tentar falsificar a sua identidade para se fazer passar por uma unidade de saúde legítima ao enviar um pedido ao Broker. Isto pode ocorrer, por exemplo, se o atacante interceptar uma comunicação legítima entre uma Aplicação Médica e o Broker e, em seguida, modificar os cabeçalhos da mensagem para falsificar a identidade da unidade de saúde. Ao fazer isto, o atacante pode enganar o Broker e obter acesso indevido a informações confidenciais dos pacientes.

Mitigação da Ameaça

Para mitigar o risco de falsificação de identidade durante a comunicação com o Broker, é fundamental implementar medidas de autenticação robustas. Uma estratégia eficaz envolve o uso de certificados digitais para autenticação mútua entre as entidades e o Broker. Isto garante que apenas entidades autorizadas tenham permissão para interagir com o sistema. Além disso, a criptografia dos dados durante a transmissão ajuda a garantir a confidencialidade e integridade das informações, reduzindo a possibilidade de falsificação de identidade durante a comunicação.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Baixa
- Risco Final - Médio

A falsificação de identidade na comunicação com o Broker apresenta um impacto Alto no sistema, pois pode resultar em acesso não autorizado a informações sensíveis do paciente ou na manipulação de dados. No entanto, a facilidade de exploração dessa vulnerabilidade é baixa, uma vez que a implementação de medidas de autenticação robustas, como certificados digitais e criptografia, dificulta a capacidade dos atacantes de falsificar identidades e aceder indevidamente ao sistema. Embora o impacto seja alto, o risco geralmente é mitigado com eficácia por meio de medidas de segurança adequadas.

2 - Falsificação de identidade na resposta do Broker

Nesta ameaça, um atacante pode tentar falsificar a identidade do Broker ao enviar uma resposta às unidades de saúde contendo informações falsas sobre os atributos dos pacientes. Por exemplo, o atacante pode criar uma entidade falsa que se passa pelo Broker e envia respostas falsificadas às unidades de saúde, fornecendo informações incorretas sobre os atributos dos pacientes. Isto pode resultar em decisões clínicas erradas ou na divulgação de informações confidenciais a terceiros não autorizados.

Mitigação da Ameaça

Para mitigar o risco de falsificação de identidade na resposta do Broker, é essencial implementar mecanismos de validação de autenticidade nas mensagens recebidas. Uma abordagem eficaz é utilizar assinaturas digitais para verificar a integridade e autenticidade das respostas do Broker. Isto envolve o uso de certificados digitais para assinar digitalmente as mensagens enviadas pelo Broker, permitindo que as entidades receptoras verifiquem a origem e a integridade dos dados recebidos. Além disso, a criptografia das comunicações pode ser empregada para proteger ainda mais as informações durante a transmissão, reduzindo o risco de falsificação de identidade e interceção de dados por partes não autorizadas.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Baixa
- Risco Final - Médio

A falsificação de identidade na resposta do Broker apresenta um impacto Alto no sistema, uma vez que pode resultar na manipulação de dados ou na divulgação não autorizada de informações confidenciais. No entanto, a facilidade de exploração desta vulnerabilidade é baixa, pois a implementação de mecanismos de validação, como assinaturas digitais, dificulta a capacidade dos atacantes de falsificar respostas do Broker. Portanto, embora o impacto seja significativo, o risco geralmente é mitigado de forma eficaz por meio de medidas de segurança adequadas.

3.3.2 Tampering - Integrity

1 - Manipulação de Dados na Comunicação com o Broker

Esta ameaça refere-se à possibilidade de um atacante manipular os dados durante a comunicação com o Broker. Por exemplo, um atacante poderia modificar os pedidos ou respostas enviadas para o Broker, alterando informações sensíveis ou inserindo dados falsos.

Mitigação da Ameaça

Como formas de mitigação para estas ameaças, deve-se implementar protocolos de comunicação seguros, como HTTPS, para garantir a integridade e confidencialidade dos dados em trânsito, utilizar assinaturas digitais para verificar a autenticidade e integridade dos dados transmitidos, envolvendo o uso de certificados digitais para assinar e verificar as mensagens e criptografar os dados sensíveis durante a transmissão para evitar a manipulação por parte de terceiros.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média
- Risco Final - Média-Alta

Esta ameaça tem um alto risco de impacto, pois a manipulação bem sucedida dos dados pode resultar em graves consequências, como a divulgação ou alteração de informações sensíveis. Em termos de facilidade de exploração, o risco é considerado médio, pois pode exigir habilidades técnicas avançadas para realizar a manipulação, mas é viável para um atacante determinado.

2 - Alteração de Mensagens no Interior do Broker

Nesta ameaça, o foco está na possibilidade de um atacante comprometer a integridade das mensagens dentro do próprio Broker. Isto pode ocorrer através da manipulação dos dados armazenados temporariamente ou em trânsito dentro do Broker, antes que sejam transmitidos para as entidades de destino.

Mitigação da Ameaça

Para mitigar a ameaça, temos de implementar controlos de integridade, como checksums ou hashes, para verificar se os dados foram modificados durante o armazenamento ou transmissão dentro do Broker, assim como utilizar mecanismos de autenticação forte para garantir que apenas entidades autorizadas possam aceder e modificar os dados dentro do Broker.

Devemos também monitorizar de perto o tráfego de dados dentro do Broker e detectar qualquer atividade suspeita ou tentativas de manipulação.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Média-Alta

A alteração de mensagens no interior do Broker apresenta um alto risco de impacto, uma vez que pode comprometer a integridade e a confiança dos dados transmitidos entre as entidades. Em termos de facilidade de exploração, o risco é considerado médio-alto, pois pode exigir conhecimentos técnicos substanciais e acesso privilegiado ao sistema do Broker para realizar com sucesso a manipulação dos dados.

3.3.3 Repudiation - Non-Repudiation

1 - Repúdio de Transações pelo Broker

Esta ameaça refere-se à possibilidade do Broker negar a ocorrência de transações ou comunicações entre as entidades, permitindo que ele ou uma das partes envolvidas negue ter realizado uma transação específica. Por exemplo, o Broker pode negar ter recebido ou transmitido determinados dados, levando a disputas de responsabilidade entre as entidades.

Mitigação da Ameaça

Como formas de mitigação, deverão ser implementados logs de auditoria detalhados que registem todas as transações e comunicações intermediadas pelo Broker. Estes logs devem incluir informações como origem, destino, horário e conteúdo das transações, tal como vimos na Aplicação do Paciente e na Aplicação Médica. Deverão também ser utilizadas as já vistas técnicas de assinatura digital para garantir a autenticidade e integridade dos registos de transações. Cada transação deve ser assinada digitalmente pelas partes envolvidas e armazenada de forma segura no Broker.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Baixa-Média
- Risco Final - Médio

A repudiação de transações pelo Broker apresenta um risco de impacto médio a alto, pois pode resultar em disputas legais ou perda de confiança nas transações intermediadas pelo sistema. Em termos de facilidade de exploração, o risco é considerado baixo a médio, pois requer acesso privilegiado ao sistema do Broker e manipulação dos registos de transações.

2 - Falsificação de Logs de Auditoria

Esta ameaça diz respeito à possibilidade de um atacante falsificar ou modificar os registos de auditoria mantidos pelo Broker para encobrir atividades maliciosas ou comprometer a integridade das transações registadas. Por exemplo, um atacante pode excluir ou modificar registos de transações para ocultar as suas ações.

Mitigação da Ameaça

Implementar controls de acesso rigorosos para garantir que apenas usuários autorizados tenham permissão para visualizar ou modificar os registos de auditoria, utilizar tecnologias de armazenamento seguro, como blockchain ou sistemas de log imutáveis, para

garantir a integridade e inviolabilidade dos registos de auditoria e realizar auditorias regulares nos registos de auditoria para detectar e investigar qualquer atividade suspeita ou inconsistência nos registos.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

A falsificação de logs de auditoria representa um risco de impacto médio-alto, pois pode comprometer a confiabilidade e a integridade das evidências de transações registadas. Em termos de facilidade de exploração, o risco é considerado médio-alto, pois pode exigir acesso privilegiado ao sistema do Broker e conhecimentos técnicos avançados para manipular os registos de auditoria sem detecção.

3.3.4 Information Disclosure - Confidentiality

1 - Divulgação não autorizada de Dados de Transações

Esta ameaça refere-se à possibilidade de divulgação não autorizada de informações confidenciais contidas nas transações intermediadas pelo Broker. Isto pode ocorrer devido a falhas de segurança no sistema do Broker ou ações maliciosas de terceiros que intercetam ou acedem indevidamente os dados em trânsito.

Mitigação da Ameaça

Para mitigar esta ameaça, será necessário implementar criptografia robusta para proteger os dados transmitidos entre as entidades e o Broker, garantindo que apenas as partes autorizadas possam aceder aos mesmos, estabelecer políticas de controlo de acesso que limitem o acesso aos dados do Broker apenas às Entidades do sistema com base em princípios de necessidade de conhecimento e a realização testes de segurança regulares, como avaliações de vulnerabilidades e testes de penetração, para identificar e corrigir quaisquer falhas de segurança no sistema do Broker.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Média
- Risco Final - Médio-Alto

A divulgação não autorizada de dados de transações apresenta um risco de impacto médio a alto, pois pode resultar na exposição de informações confidenciais das entidades envolvidas. Em termos de facilidade de exploração, o risco é considerado médio, pois pode exigir conhecimentos técnicos avançados para intercetar ou aceder aos dados de transações sem autorização.

2 - Exposição de Dados Sensíveis nos Logs de Auditoria

Esta ameaça envolve a possibilidade de que dados sensíveis contidos nos logs de auditoria mantidos pelo Broker sejam expostos a utilizadores não autorizados. Isto pode ocorrer devido a configurações inadequadas de segurança ou falhas no controlo de acesso aos registos de auditoria.

Mitigação da Ameaça

Implementar mecanismos de mascaramento de dados nos registos de auditoria para ocultar informações sensíveis, como dados pessoais ou financeiros, de utilizadores não autorizados, aplicar rigorosos controlos de acesso aos logs de auditoria, garantindo que apenas utilizadores autorizados tenham permissão para visualizar ou aceder a informações sensíveis contidas nos registos e realizar auditorias periódicas nos registos de auditoria para identificar e corrigir quaisquer vulnerabilidades ou exposições de dados sensíveis.

Análise de Risco

- Impacto - Médio
- Facilidade de Exploração - Média
- Risco Final - Médio

A exposição de dados sensíveis nos logs de auditoria apresenta um risco de impacto médio, pois pode resultar na divulgação não autorizada de informações confidenciais das entidades envolvidas. Em termos de facilidade de exploração, o risco é considerado médio, pois pode exigir acesso privilegiado ao sistema do Broker e conhecimentos específicos sobre a estrutura e o formato dos logs de auditoria para identificar e aceder a dados sensíveis.

3.3.5 Denial of Service - Availability

1 - Ataques de Negação de Serviço Distribuído contra o Broker

Esta ameaça envolve a possibilidade de um ataque coordenado de negação de serviço direcionado ao Broker, visando sobrecarregar os seus recursos e torná-lo inacessível para o armazenamento de logs da parte da Aplicação do Paciente e para receber e responder aos pedidos da Aplicação Médica. Os ataques DDoS podem ser realizados por meio de uma rede de computadores comprometidos, conhecidos como botnets, que enviam uma grande quantidade de tráfego malicioso para o Broker.

Mitigação da Ameaça

Como formas de mitigação para esta ameaça, devemos implementar sistemas de detecção e prevenção de intrusões (IDS/IPS) para identificar e bloquear atividades suspeitas que possam indicar um ataque DDoS em andamento.

Devemos também utilizar serviços de mitigação de DDoS oferecidos por "cloud security providers"para filtrar e mitigar o tráfego malicioso antes que ele atinja o Broke, assim como dimensionar adequadamente os recursos de rede e hardware do Broker para lidar com picos de tráfego e ataques DDoS, garantindo assim a disponibilidade contínua dos serviços.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final - Médio-Alto

Os ataques DDoS representam um risco significativo de impacto alto, pois podem resultar na interrupção total ou parcial dos serviços oferecidos pelo Broker, causando prejuízos financeiros e danos à reputação. Em termos de facilidade de exploração, o risco é considerado médio-alto, pois os ataques DDoS podem ser executados com relativa facilidade por meio de ferramentas automatizadas disponíveis na internet, embora a mitigação eficaz possa exigir recursos técnicos avançados e investimentos significativos.

2 - Sobrecarga de Solicitações Legítimas ao Broker

Esta ameaça envolve a possibilidade de sobrecarregar os recursos do Broker devido a uma carga excessiva de solicitações legítimas de utilizadores autorizados. Isto pode ocorrer devido a eventos inesperados, como picos de tráfego ou atividades de processamento intensivo, que excedem a capacidade do sistema do Broker.

Mitigação da Ameaça

Para mitigação, devemos implementar políticas de limitação da taxa de solicitações para controlar o número de solicitações que podem ser processadas pelo Broker num determinado período de tempo, evitando assim sobrecargas de recursos, utilizar técnicas de balanceamento de carga para distribuir uniformemente as solicitações entre vários servidores do Broker, garantindo uma distribuição equitativa da carga e evitando a sobrecarga de servidores individuais e monitorizar proativamente o desempenho e a utilização dos recursos do Broker para identificar e mitigar rapidamente qualquer anomalia ou comportamento anormal que possa indicar uma possível sobrecarga iminente.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Média
- Risco Final - Médio

A sobrecarga de solicitações legítimas apresenta um risco de impacto médio-alto, pois pode resultar na degradação ou interrupção dos serviços oferecidos pelo Broker, afetando negativamente a experiência dos utilizadores e a reputação da plataforma. Em termos de facilidade de exploração, o risco é considerado médio, pois pode ser desencadeado por eventos legítimos, como picos de tráfego sazonal, que podem ser mais complicados de prever e mitigar.

3.3.6 Elevation of Privilege - Authorization

1 - Elevação de Privilégios no Sistema do Broker

Esta ameaça refere-se à possibilidade de um atacante obter acesso não autorizado a recursos privilegiados ou funcionalidades do sistema do Broker, permitindo-lhe realizar ações que normalmente não teria permissão para executar. Isto pode incluir a manipulação indevida de dados sensíveis, a execução de comandos maliciosos ou a obtenção de controlo total sobre o sistema do Broker.

Mitigação da Ameaça

Implementar controlo de acesso granular para restringir os privilégios de utilizadores e Aplicações no sistema do Broker, garantindo que apenas as operações autorizadas sejam permitidas, aplicar princípios de segregação de funções para limitar o acesso a recursos e funcionalidades com base no papel e na responsabilidade das Entidades, reduzindo assim a superfície de ataque para potenciais vetores de exploração e utilizar mecanismos de monitorizaçãoo e detecção de intrusões para identificar atividades suspeitas ou tentativas de elevação de privilégios no sistema do Broker, permitindo uma resposta rápida e eficaz a possíveis violações de segurança.

Análise de Risco

- Impacto - Alto
- Facilidade de Exploração - Média-Alta
- Risco Final -

A elevação de privilégios no sistema do Broker representa um risco de impacto alto, pois pode resultar no comprometimento da integridade, confidencialidade e disponibilidade dos dados armazenados e processados pelo sistema. Em termos de facilidade de exploração, o risco é considerado médio-alto, dependendo das vulnerabilidades específicas presentes no sistema e da habilidade do atacante em explorá-las.

2 - Manipulação de Dados de Autorização no Broker

Esta ameaça refere-se à possibilidade de um atacante manipular indevidamente os dados de autorização armazenados no sistema do Broker para conceder acesso não autorizado a recursos ou funcionalidades a utilizadores não privilegiados. Isto pode incluir a modificação de atributos de autorização, a falsificação de certificados ou a criação de contas de utilizador falsas para obter acesso indevido ao sistema.

Mitigação da Ameaça

Como formas de mitigação, temos a implementação de controlos de integridade e autenticidade para os dados de autorização armazenados no sistema do Broker, garantindo que estes não possam ser alterados ou manipulados por entidades não autorizadasm, implementar técnicas de criptografia e assinatura digital para proteger os dados de autorização em trânsito e em repouso, impedindo assim a interceção ou adulteração dos mesmos por parte de atacantes e adotar práticas de gestão de identidade e acesso robustas, como autenticação multifator.

Análise de Risco

- Impacto - Médio-Alto
- Facilidade de Exploração - Média
- Risco Final - Médio

A manipulação de dados de autorização no Broker representa um risco de impacto médio-alto, pois pode resultar na concessão indevida de acesso a recursos sensíveis ou confidenciais, comprometendo assim a segurança e a privacidade dos dados do sistema. Em termos de facilidade de exploração, o risco é considerado médio, pois pode exigir um conhecimento avançado do sistema e das suas vulnerabilidades específicas por parte do atacante, sendo atribuído um risco final de Médio.

4 Catalogação de Vulnerabilidades e Exploits

4.1 Aplicação do Paciente; Aplicação Médica; Base de Dados; Autoridade Certificadora

Para estas Entidades, não será possível, nesta fase, fazer uma catalogação das vulnerabilidades, uma vez que ainda não se encontram definidos os softwares e as suas respetivas versões a utilizar para a implementação dos objetivos que se pretendem atingir. Tendo isto em conta, a modelação de ameaças feita na secção anterior é, neste momento, a única forma de avaliar as potencias ameaças para a infraestrutura no que diz respeito a estas Entidades.

4.2 Broker

No que diz respeito ao sistema do Broker, é-nos dito que a sua composição actual é a seguinte:

- Sistema Operativo - Ubuntu Server 20.04.6 LTS
- Servidor Web - Apache Tomcat 10.0.27
- Base de Dados - PostgreSQL 14.11
- Biblioteca de Comunicação Segura - OpenSSL 3.0.13
- Backend de Gestão - Django 5.0.3

Com esta informação, vamos identificar as vulnerabilidades e exploits conhecidas com mais impacto para estes componentes, de maneira a verificar se será necessário optar por outras soluções, fazer algum tipo de atualização de versões, alterar as configurações do software ou se estes se encontram de acordo com o que é esperado para garantir que o sistema se encontra com o nível de segurança desejado.

4.2.1 Sistema Operativo - Ubuntu Server 20.04.6 LTS

Em primeiro lugar, temos o Sistema Operativo, em que este corresponde ao Ubuntu Server 20.04.6 LTS. Esta versão foi lançada a 23 de Março de 2023 e é a versão com Long-Term Support até Abril de 2025, tal como todas as outras versões dentro da release 20.04.

Tal como seria de esperar, a maior parte das vulnerabilidades encontradas correspondem a vulnerabilidades em serviços a correr no sistema e não no SO especificamente, sendo que a maioria delas afeta qualquer uma das versões do Ubuntu Server dentro das releases 20.04.*.

Posto isto, como vulnerabilidades para a versão 20.04 do Ubuntu, foram encontradas as seguintes:

CVE-2020-1472

A vulnerabilidade CVE-2020-1472, também conhecida como "Zerologon", é uma vulnerabilidade crítica que afeta o protocolo de autenticação Netlogon no Windows Server.

Esta vulnerabilidade permite que um atacante não autenticado obtenha controlo total sobre um domínio do Windows Server ao explorar uma falha no algoritmo de criptografia utilizado pelo Netlogon. Ao explorar esta falha, um atacante pode falsificar identidades de computadores no domínio, permitindo o acesso não autorizado a sistemas e informações confidenciais.

O impacto desta vulnerabilidade é extremamente grave, pois um atacante pode comprometer completamente a segurança de uma rede, ganhando acesso total a sistemas, bases de dados e outros recursos protegidos. Além disso, a exploração bem-sucedida da vulnerabilidade pode permitir que o atacante permaneça não detetado por longos períodos de tempo.

Como medida de mitigação, a Microsoft lançou patches de segurança para corrigir esta vulnerabilidade, pelo que é altamente recomendável que o sistema do Broker a utilizar o Ubuntu Server 20.04.* aplique estes patches o mais rápido possível para se proteger contra possíveis ataques. Além disso, outras medidas de segurança, como monitorização de rede e segmentação de rede, podem ajudar a mitigar os riscos associados a esta vulnerabilidade.

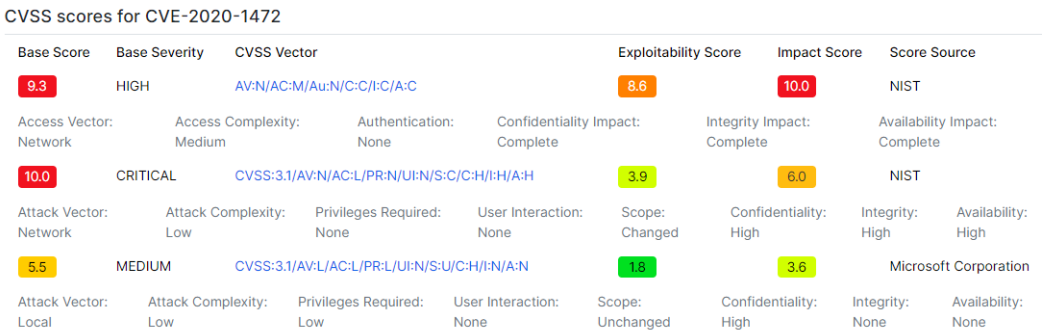


Figura 4.1: Vulnerabilidade CVE-2020-1472

CVE-2020-12284

A vulnerabilidade CVE-2020-12284 afetou o FFmpeg, uma biblioteca multimédia que é amplamente utilizada para decodificar, codificar, transcodificar e reproduzir ficheiros de

áudio e vídeo em diferentes formatos. Esta vulnerabilidade foi identificada em versões específicas do FFmpeg, nomeadamente a versão 4.1 e a versão 4.2.2.

O problema ocorreu devido a uma falha no tratamento de marcações JPEG_MARKER_SOS na função cbs_jpeg_split_fragment no ficheiro cbs_jpeg.c. Esta falha resultou num desbordamento de buffer baseado na pilha durante o processamento, devido à ausência de verificação de comprimento adequada.

Esta vulnerabilidade permitiu a um atacante explorar a falha manipulando um ficheiro de vídeo ou áudio especialmente concebido, levando a uma execução de código arbitrário ou a uma condição de negação de serviço no sistema afetado.

Para mitigar esta vulnerabilidade, tendo em conta que esta afeta os sistemas com Ubuntu Server 20.04.*, é aconselhado que se a atualize para uma versão mais recente do FFmpeg que contém as correções de segurança necessárias. Além disso, recomenda-se evitar a reprodução ou manipulação de ficheiros multimédia não confiáveis de fontes desconhecidas para reduzir o risco de exploração desta vulnerabilidade.

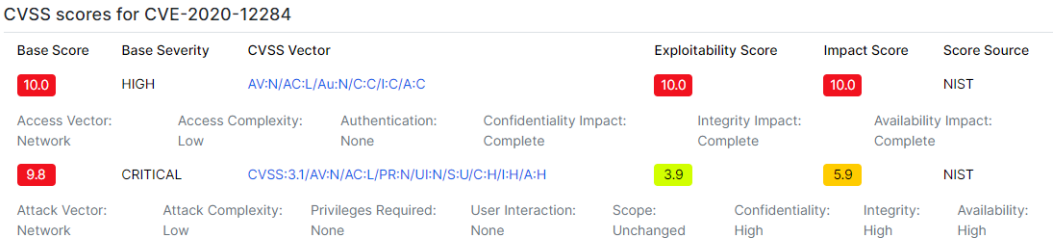


Figura 4.2: Vulnerabilidade CVE-2020-12284

CVE-2020-12395

A vulnerabilidade CVE-2020-12395 afetou o Firefox e ocorreu devido a uma falha no motor JavaScript do Firefox ao manipular objetos do tipo BigInt. Esta falha poderia levar a um vazamento de memória, o que poderia ser explorado por um atacante remoto para obter informações sensíveis ou causar uma condição de negação de serviço no navegador afetado.

Esta vulnerabilidade poderia ser explorada através da execução de código JavaScript malicioso numa página da web, levando à execução não autorizada de código ou à interrupção do funcionamento normal do navegador.

Para mitigar essa vulnerabilidade, é aconselhado a atualização do Firedox para uma versão mais recente do navegador, que contém as correções de segurança necessárias.

4.2.2 Servidor Web - Apache Tomcat 10.0.27

Para o Apache Tomcat, a situação é bastante diferente do Ubuntu Server. Esta é uma versão mais antiga, considerada numa situação "end of life", o que significa que já não tem qualquer suporte. Vulnerabilidades reportadas para esta versão depois de 31 de Outubro de 2022 não serão corrigidas pelo que a decisão correta será a de mudar para a

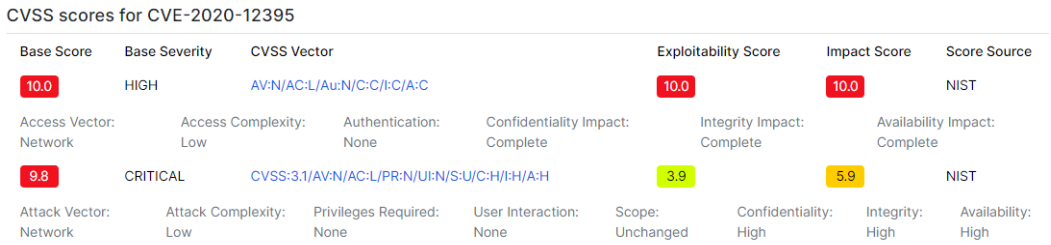


Figura 4.3: Vulnerabilidade CVE-2020-12395

versão 10.1.x, que corresponde à versão suportada pela comunidade do Apache Tomcat. Esta alteração fará com que eventuais vulnerabilidades encontradas no servidor sejam corrigidas, mantendo a segurança do serviço.

No entanto, e caso a equipa pretenda manter a versão 10.0.27 do Apache Tomcat, é importante ressaltar que o as bases de dados de vulnerabilidades existentes não indicam a ocorrência de qualquer vulnerabilidade para a versão especificada, sendo apenas apresentada uma vulnerabilidade na própria plataforma do Apache Tomcat, tendo esta sido corrigida em 2022:

CVE-2022-34305

Para esta vulnerabilidade, se o Tomcat estivesse configurado para ignorar cabeçalhos HTTP inválidos, através da definição de rejectIllegalHeader como false (não o padrão), o Tomcat não rejeitaria um pedido contendo um cabeçalho Content-Length inválido, tornando possível um ataque de smuggling de pedido se o Tomcat estivesse localizado atrás de um proxy reverso que também falhasse em rejeitar o pedido com o cabeçalho inválido.

Esta foi considerada uma vulnerabilidade de risco médio.

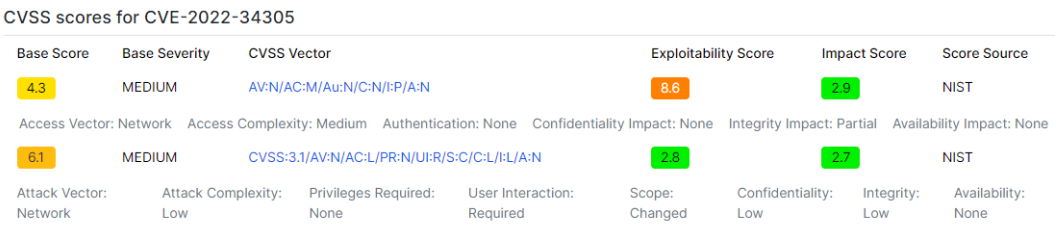


Figura 4.4: Vulnerabilidade CVE-2022-34305

4.2.3 Base de Dados - PostgreSQL 14.11

A versão 14.11 do PostgreSQL foi lançada a 27 de Setembro e o seu suporte acaba apenas a 12 de Novembro de 2026. Para esta versão em específico, existe apenas uma vulnerabilidade conhecida, mais especificamente a CVE-2024-0985, que faz com que seja aconselhável a escolha de uma versão mais recente, tal como será explicado de

seguida. Mesmo sem a existência desta vulnerabilidade, seria ideal a troca para uma versão mais recente, uma vez que normalmente estas vêm com correções de segurança, novos recursos, melhorias de desempenho e correções de bugs.

No que diz respeito à vulnerabilidade encontrada:

CVE-2024-0985

A vulnerabilidade CVE-2024-0985 para o PostgreSQL refere-se a um problema de segurança relacionado com a funcionalidade "REFRESH MATERIALIZED VIEW CONCURRENTLY". Esta vulnerabilidade permite que o criador de um objeto execute funções SQL arbitrárias como o emissor de comandos com o objetivo de executar funções SQL como o proprietário da view materializada, possibilitando a atualização segura de views materializadas não confiáveis. O ataque requer atrair a vítima para executar REFRESH MATERIALIZED VIEW CONCURRENTLY na view materializada do atacante. Como parte da exploração desta vulnerabilidade, o atacante cria funções que utilizam o "CREATE RULE"para converter a tabela temporária internamente construída numa view.

Para segurança e para evitar o exploit desta vulnerabilidade por um atacante, é recomendada a atualização da versão do PostgreSQL para a versão 16 ou posterior, uma vez que a mesma não funciona nestas versões.

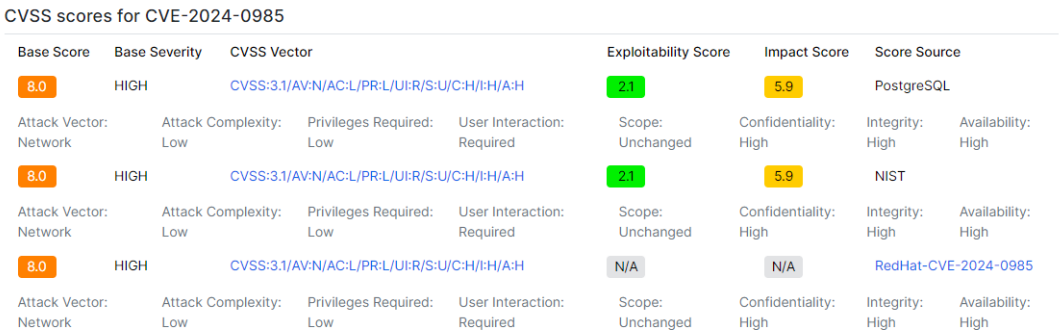


Figura 4.5: Vulnerabilidade CVE-2024-0985

4.2.4 Biblioteca de Comunicação Segura - OpenSSL 3.0.13

Para o OpenSSL, é utilizada a versão 3.0.13, sendo que a versão 3.0 é a versão LTS neste momento, sendo suportada até 7 de Setembro de 2026. Para as versões 3.0.*, existe apenas uma versão posterior, a 3.0.14 que vem corrigir a única vulnerabilidade encontrada, a CVE-2024-2511. Tendo isto em conta, seria recomendado fazer um upgrade para a versão 3.0.14, apesar de que o risco de exploração da mesma é extremamente baixo. No que diz respeito á vulnerabilidade, foi encontrado o seguinte:

CVE-2024-2511

Esta vulnerabilidade pode ocorrer no TLSv1.3 se a opção SSL_OP_NO_TICKET não padrão estiver a ser usada (mas não se o suporte a early_data também estiver configurado e a proteção anti-replay padrão estiver em uso). Neste caso, sob certas condições, a cache de sessões pode entrar num estado incorreto e não ser limpa adequadamente à medida que se enche. A cache de sessões continuará a crescer de forma ilimitada fazendo com que um atacante possa criar deliberadamente o cenário para esta falha para forçar uma negação de serviço. Também pode ocorrer por acidente durante a operação normal.

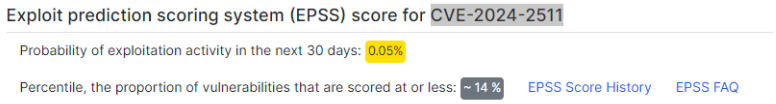


Figura 4.6: Vulnerabilidade CVE-2024-2511

4.2.5 Backend de Gestão - Django 5.0.3

Para o Backend de Gestão é utilizado o Django, mais especificamente a versão 5.0.3. Após uma consulta das releases do Django na sua plataforma, a versão 5.0.3 vem corrigir a vulnerabilidade CVE-2024-27351. É possível observar também a existência de duas versões posteriores à 5.0.3, nomeadamente a 5.0.4 e a 5.0.5. Tal como vimos até agora, seria indicada a alteração para uma versão mais recente, especialmente tendo em conta que a versão 5.0.4 corrige vários bugs que afetam a performance, não havendo no entanto uma razão aparente para a escolha da versão 5.0.5 neste momento.

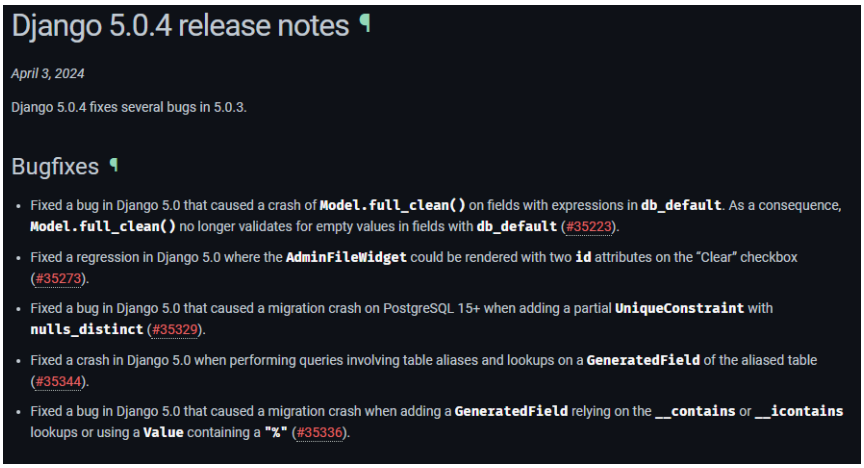


Figura 4.7: Bugfixes na versão 5.0.4

5 Conclusão

5.1 Conclusões e Considerações Finais

Ao longo deste relatório, foram identificadas e analisadas diversas ameaças de segurança presentes no sistema de Saúde dado, utilizando o modelo STRIDE como base para a modelação de ameaças e utilizando diversas bases de dados de vulnerabilidades para o estudo das vulnerabilidades e exploits presentes no sistema do Broker. Cada ameaça foi detalhadamente descrita, incluindo uma análise de risco que considerou o impacto e a facilidade de exploração. Com base nessas análises, foram propostas medidas de mitigação para fortalecer a segurança dos sistemas e proteger os dados dos pacientes.

É importante destacar a complexidade e a diversidade das ameaças identificadas, demonstrando a necessidade de uma abordagem abrangente e proativa para garantir a segurança da informação no contexto da saúde digital. As medidas de mitigação propostas visam não apenas lidar com as ameaças existentes, mas também prevenir futuros ataques e garantir a autenticidade, integridade, confidencialidade e disponibilidade dos dados dos pacientes.

5.2 Trabalho Futuro

Como trabalho futuro, recomenda-se a implementação e o teste das medidas de mitigação propostas para avaliar a sua eficácia na redução do risco de segurança. Além disso, é essencial realizar avaliações periódicas de segurança e atualizações regulares nos sistemas para lidar com novas ameaças e vulnerabilidades que possam surgir. O treino contínuo dos profissionais de saúde e o envolvimento dos pacientes na promoção da segurança da informação também são aspectos importantes a serem considerados no trabalho futuro. Por fim, a colaboração entre instituições de saúde, desenvolvedores de software e especialistas em segurança cibernética é fundamental para garantir a proteção adequada dos dados médicos e pessoais dos pacientes num ambiente digital em constante evolução.