Faculdade Adventista
BAHIA

Relatório de Análise de Vulnerabilidades

Orientador: Jean do Ouro

Classificação: PÚBLICA

Última Revisão: 01/12/2022

CONTEÚDO

Sumário

1. SUMÁRIO EXECUTIVO

Este relatório reflete os resultados da análise de vulnerabilidades da plataforma (aplicações web) Unity Technologies (www.unity3d.com). A análise de vulnerabilidade foi realizada no período de 17 de novembro a 01 de dezembro de 2022.

leandro2002rc@gmail.com
samysdantas@gmail.com

1.1 Sobre Projeto de Desenvolvimento Profissional

Projeto desenvolvido pelos alunos da Faculdade Adventista da Bahia que consiste em encontrar vulnerabilidades em aplicações web das empresas que participam do programa da Bugcrowd, uma plataforma de segurança coletiva mais inteligente da indústria, e que utiliza a Crowdsourced Security como ferramenta para eliminar o desequilíbrio, aproveitando os pesquisadores de segurança do Whitehat para encontrar e eliminar vulnerabilidades.

1.2 Código de Ética

Os alunos graduando do Curso de Gestão da Tecnologia da Informação da Faculdade Adventista da Bahia aplicam e mantêm os seguintes princípios:

• Integridade: a integridade dos pentesters estabelece confiança e, portanto, fornece a base para a confiança em seu julgamento;

• Objetividade: os pentesters possuem o mais alto nível de objetividade profissional na coleta, avaliação e comunicação de informações sobre a atividade ou processo que está sendo examinado, fazendo uma avaliação equilibrada de todas as circunstâncias relevantes para suas análises e não são indevidamente influenciados por seus próprios interesses ou por outros na formação de julgamentos;

• Confidencialidade: os pentesters respeitam o valor e a propriedade das informações que recebem e não divulgam informações sem a devida autoridade, a menos que haja uma obrigação legal ou profissional de fazê-lo;

• Competência: os pentesters aplicam os conhecimentos, habilidades e experiência necessários no desempenho dos serviços de análise de vulnerabilidades e testes de intrusão.

2. INTRODUÇÃO

Foi realizado análises de vulnerabilidades na plataforma Unity, conforme definido no "Escopo" deste relatório, cujos resultados serão abordados adiante.

Os testes de segurança foram realizados no período de 17/11/2022 a 01/12/2022 e seu objetivo foi identificar vulnerabilidades e propor recomendações para sua correção.

As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

2.1 Termo de responsabilidade

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente, quanto pelo que foi estabelecido pelo orientador Jean Ouro.

As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de “Escopo” e “Objetivos” e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades.

Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.

Neste contexto, embora tenham sido feitos todos os esforços para auditar e avaliar a segurança do ambiente computacional da Unity, este relatório não garante de forma alguma o estabelecimento de um sistema impenetrável. Sendo assim, a FADBA e os pentesters não se responsabilizam por qualquer perda ou dano direto ou indireto causado por qualquer falha ou violação dos sistemas desta da plataforma de viagem.

Por fim, as informações deste relatório têm classificação PÚBLICA e devem ser usadas apenas pela Unity e pela FADBA, sendo de inteira e única responsabilidade de ambas.

2.1 Análise da organização

A Unity Technologies é uma desenvolvedora de Software de jogos eletrônicos sediada em San Francisco, Califórnia.

Fundada em 2004 na Dinamarca, tinha como nome Over the Edge Entertainment (OTEE) e mudou seu nome para Unity Technologies em 2007.

leandro2002rc@gmail.com
samysdantas@gmail.com

A Unity Technologies é mais conhecida pelo desenvolvimento da Unity, um motor de jogo usado para desenvolver jogos e aplicativos.

2.2 Objetivo

O objetivo dos testes foi fornecer informações confiáveis sobre a segurança do ambiente computacional da Unity. Dessa forma, a avaliação identificou vulnerabilidades e quantificou sua criticidade, para que as mesmas possam ser geridas, resolvidas e, consequentemente, ajudar a prevenir o mau funcionamento e/ou perda financeira por meio de fraudes, fornecer diligências a regulações a clientes, e proteger a marca contra a perda de reputação.

2.3 Escopo

Os testes realizados foram do tipo “White Box” e seguiram uma abordagem com base nos limites impostos pela empresa. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise. Ademais, foram reunidas informações sobre a organização para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de segurança da informação. Nesse sentido, foram realizados testes básicos de verificação de segurança em IPs obtidos indiretamente, isto é, IPs que são públicos e que foram conseguidos através de consulta ao “DNSdumpster” - ferramenta de pesquisa de domínio gratuitos que visam descobrir hosts relacionados a um domínio, conforme mostrados na Figura 1.

Figura 1 - Mapeamento dos endereços IP para o domínio “www.unity3d.com”

leandro2002rc@gmail.com
samysdantas@gmail.com

2.4 Limites

Todos os devidos cuidados foram tomados com base na especificação e critérios da empresa (Unity) e as orientações do professor (Jean do Ouro) para não prejudicar o funcionamento da empresa, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma.

Não fazem parte do escopo: Negação de serviço, Problemas de limitação de taxa, Spamming, Falsificação de e-mail, Engenharia social (incluindo phishing) de funcionários ou contratados da Unity, Quaisquer tentativas físicas contra propriedades ou data centers da Unity, Auto-XSS e problemas exploráveis apenas por auto-XSS, problemas relacionados ao window.opener,

Problemas de segurança de cookies para cookies sem sessão, Segurança do cabeçalho HTTP, Questões profundas de defesa, Entrar/Sair CSRF, Relatórios automatizados de ferramentas, Presença de preenchimento automático em formulários da web, Ataques exploráveis apenas em navegadores mais antigos ou navegadores com configurações não padrão, Redirecionamentos abertos (a menos que possam ser usados para roubar tokens ativamente), Relatórios informando que o software está desatualizado ou vulnerável sem uma prova de conceito, Preocupações com as melhores práticas sem uma demonstração de explorabilidade prática, Formulários de contato e suporte , Injeção de HTML que não leva a XSS.

3 DETALHAMENTO DOS SOFTWARES INSTALADOS

ANÁLISE E RASTREAMENTO

Insights de domínio do Facebook	Mixpanel	Insights de domínio do Facebook	Eloqua
Google Optimize 360	New Relic	Google Universal Analytics	Google Analytics

WIDGETS

Sajari	Apple Whitelist	OneTrust	Optanon	Dropbox Business	Smartsheet

MongoDB	Google Custom Search	Google Font API	Google Tag Manager	COVID-19	DocuSign

FRAMEWORKS

Adobe Enterprise Cloud	Bug Bounty	PHP	Organization Schema	Java EE

REDE DE DISTRIBUIÇÃO DE CONTEÚDO

UNPKG	API de bibliotecas AJAX	Akamai

MOBILE

Viewport Meta	Compatível com iPhone / Celular	Mobile Optimized	Compatível com Apple Mobile Web App

AUDIO/VIDEO MEDIA

Vidyard	Youtube	VideoJS	Youtube IFrame API

SISTEMA DE GERENCIAMENTO DE CONTEÚDO

Favro	My Salesfrorce	Drupal

JAVASCRIPT LIBRARIES AND FUNCTIONS

Bootstrap.js	html5shiv	Facebook for Websites	Modernizr
JQuery hospedado pelo Google	Vue	core-js	Moment JS

Verified Link

Facebook	Twitter	Linkedin	Instagram

SERVER NAME

Akamai DNS

WEB HOSTING PROVIDERS

Many Subdomains	Softlayer	Akamai Hosted
Google	Google Cloud	Liquid Web

EMAIL HOSTING PROVIDERS

Maligun	Zendesk	Valimail	Google Apps for Business
SPF	Eloqua Mail	Microsoft Azure DNS	DMARC

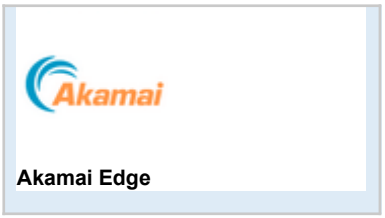
SSL CERTIFICATES

SSL por padrão	DigiCert SSL

WEB SERVERS

nginx	Verniz	Apache

CDN VERIFIED



Akamai Edge

Web Master Registration

Google Webmaster	Naver Webmaster Tools	Yandex Verification

4 METODOLOGIA

As etapas a seguir, foram conduzidas para fornecer uma avaliação dos riscos com base na norma ABNT NBR ISO/IEC 27005:2011 com intuito de determinar eventos que possam causar uma perda potencial e auxiliar na adequação dos controles de segurança do ambiente testado:

- **Identificação de Ameaças:** identificar ameaças e potenciais de comprometer ativos (como informações, processos e sistemas);
- **Identificação de Vulnerabilidade:** analisar vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos;
- **Determinação do nível das Vulnerabilidades:** A análise das vulnerabilidades é baseada nas consequências e na probabilidade de um cenário de incidente e suas consequências.
- **Avaliação das consequências:** determinar medidas apropriadas através do entendimento das vulnerabilidades por meio análise dos riscos para a tomada de decisões sobre ações futuras.

4.1 Identificação de Ameaças

A primeira fase da avaliação concentrou-se na coleta, análise e estruturação de informações sobre os itens do escopo, utilizando principalmente técnicas de análise passiva, além de normas, fontes públicas como sites, blogs e mecanismos de pesquisa, que foram consultadas para obtenção e reconhecimento de informações sobre o ambiente testado. Isso é feito para coletar informações necessárias para conduzir as demais fases dos testes. Vale ressaltar que uma ameaça pode surgir de dentro ou de fora da organização e isso significa que nenhuma ameaça será ignorada. Dessa forma, as ameaças foram identificadas genericamente e classificadas de acordo com a sua gravidade percebida.

4.2 Identificação das Vulnerabilidades

Testes automatizados e manuais foram combinados para confirmar a maioria das vulnerabilidades potenciais. Pois, uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Sendo assim, ao testar de diferentes formas os aspectos críticos, as falhas de segurança que não foram descobertas por determinado método puderam ser encontradas e avaliadas conforme o CVSS (Common Vulnerability Scoring System).

4.3 Determinação do nível das Vulnerabilidades

A análise das vulnerabilidades designa valores para a probabilidade e para as consequências de um risco. Esses valores (com base CVSS) foram atribuídos aos resultados das análises manuais e automatizadas verificando quanto à sua integridade e razoabilidade a fim de se diminuir o risco de vulnerabilidades não identificadas (falsos negativos) para um nível aceitável. Com isso, as descobertas foram avaliadas e reavaliadas individualmente para verificar se elas representavam, de fato, vulnerabilidades.

4.4 Avaliação das consequências

O relatório foi construído com base no escopo que a empresa Tamedia disponibilizou no site da Bugcrowd.com. Para as futuras decisões a serem tomadas convém que as consequências, a probabilidade e o grau de confiança na identificação e determinação do nível das vulnerabilidades

também sejam considerados. Por fim, é importante ressaltar que foi seguido à risca o que foi solicitado e todo o progresso geral com informações sobre a realização dos testes juntamente com os resultados da avaliação foram aqui documentados e serão entregues na forma deste relatório.

4.5 Ferramentas Utilizadas

- **DNSdumpster.com:** é uma ferramenta GRATUITA de pesquisa de domínio que pode descobrir hosts relacionados a um domínio. E encontrar hosts visíveis da perspectiva dos invasores é uma parte importante do processo de avaliação de segurança.
- **NMAP:** é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características.
- **BuiltWith -** é uma ferramenta de criação de perfil de website, geração de leads, análise competitiva e inteligência de negócios que fornece adoção de tecnologia, dados de comércio eletrônico e análise de uso para a internet.O rastreamento da tecnologia BuiltWith inclui widgets, análises, estruturas, sistemas de gerenciamento de conteúdo, anunciantes, redes de distribuição de conteúdo, padrões da web e servidores da web.
- **Nessus:** definido pela Tenable como a solução número um de avaliação de vulnerabilidades para profissionais de segurança. Tendo como característica a precisão Six Sigma, apresentando a menor taxa de falso-positivos do setor. Possui ampla e profunda cobertura, com mais de 56 mil CVEs (Common Vulnerabilities and Exposures) e mais

de 142 mil plugins já publicados e com crescimento exponencial voltado para a identificação de vulnerabilidades.

5 EQUIPE TÉCNICA

NOME	RESPONSABILIDADE	CONTATO
Leandro Rocha de Carvalho	Reconhecimento do ambiente, Teste, elaboração de conceitos e produção do relatório.	leandro2002rc@gmail.com
Brian Samuel de Souza Dantas	Reconhecimento do ambiente, Teste, elaboração de conceitos e produção do relatório.	samysdantas@gmail.com

6 CRONOGRAMA DE ATIVIDADES

ATIVIDADE	DATA DA REALIZAÇÃO
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo.	17 de novembro de 2022
Provas de conceito e conclusão dos testes.	20 de novembro de 2022
Avaliação de riscos e esboço do relatório.	24 de novembro de 2022
Conclusão e revisão final do relatório	29 de novembro de 2022

7 NÍVEIS DE CRITICIDADE

Para categorizar o impacto e a exploração de vulnerabilidades, os níveis de criticidade usados na seção “Vulnerabilidades Encontradas” estão de acordo com a Versão 3 do Common Vulnerability Scoring System (CVSS v3) do NIST, o qual utiliza a pontuação básica composta pelo tipo de acesso, a complexidade de acesso e o nível de autenticação exigido para explorar uma determinada vulnerabilidade, bem como o impacto relacionado à confidencialidade, integridade e disponibilidade. A pontuação aplicada às vulnerabilidades varia de 0 a 10 pontos e é normalizada categorizando-as em níveis críticos, altos, médios e baixos de criticidade.

- **Vetor de Acesso (AV):** descreve a fonte necessária de ataque para explorar uma vulnerabilidade, cujos valores possíveis são Local (L), Rede Adjacente (A) ou Rede (N);

- **Complexidade do Acesso (AC):** está relacionado à complexidade das condições que precisam estar em vigor para uma exploração bem-sucedida. Os valores possíveis são Alto (H), Médio (M) e Baixo (L);
- **Autenticação (AU):** refere-se aos níveis de autenticação que um invasor precisa transmitir para explorar uma vulnerabilidade. Os valores possíveis são Requer Várias Instâncias (M), Requer Instância Única (S) e Nenhum Requerido (N);
- **Confidencialidade (C), Integridade (I), Disponibilidade (A):** quando há impacto na confidencialidade, integridade ou disponibilidade, e cujos possíveis valores são Nenhum (N), Parcial (P) e Completo (C).

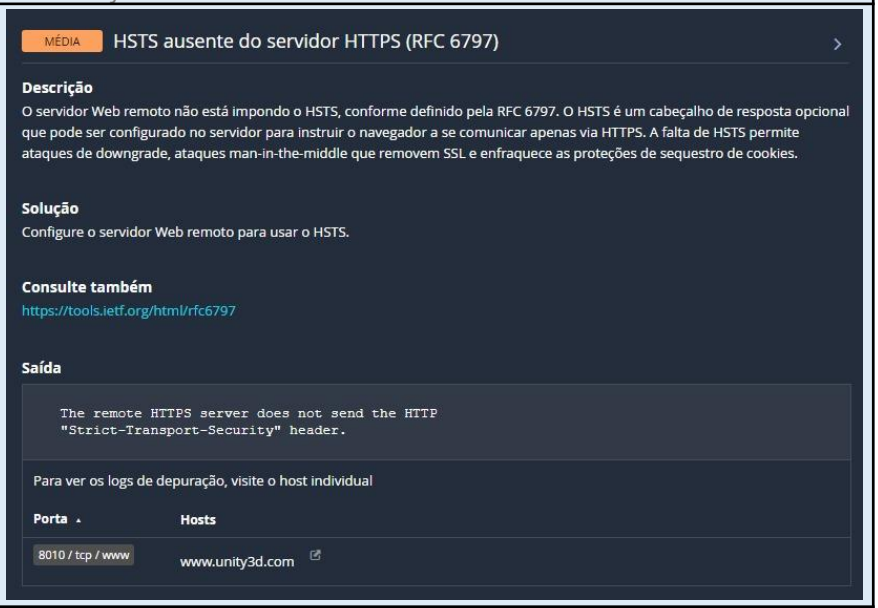
Diante do exposto, os níveis de criticidade definidos podem ser visualizados na Tabela 1, a seguir, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados para representar o risco e a criticidade calculados para cada uma das vulnerabilidades que foram identificadas.

Tabela 1 - Níveis de criticidade e descrição.

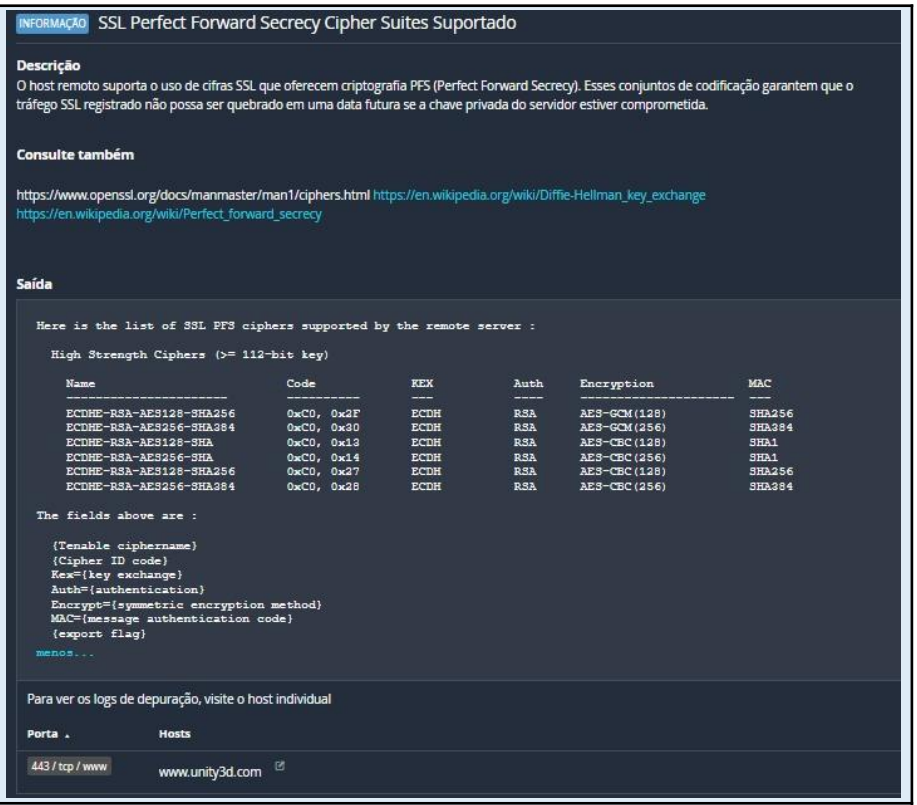
CRITICIDADE	DESCRIÇÃO
Crítica	• Pontuação Base do CVSS: 9 a 10 pontos; • Exploração trivial; • Perda de confidencialidade, integridade e disponibilidade. **A remediação imediata é crítica para os negócios.**
Alta	• Pontuação Base do CVSS: de 6 a 8.9 pontos; • Exploração quase trivial; • Perda ou de confidencialidade, ou de integridade ou de disponibilidade. **A remediação é crítica para os negócios.**
Média	• Pontuação Base do CVSS: de 4 a 6.9 pontos; • Exploração possível e comum, mas requer habilidades; • Sério impacto na confidencialidade, integridade e disponibilidade. **Ações corretivas são exigidas dentro de um prazo razoável.**
Baixa	• Pontuação Base do CVSS: de 0.1 a 3.9 pontos; • Exploração possível, mas difícil e improvável; • Impacto mensurável na confidencialidade, integridade e disponibilidade. **Ações corretivas são recomendadas.**
Informativa	**Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.**

leandro2002rc@gmail.com
samysdantas@gmail.com

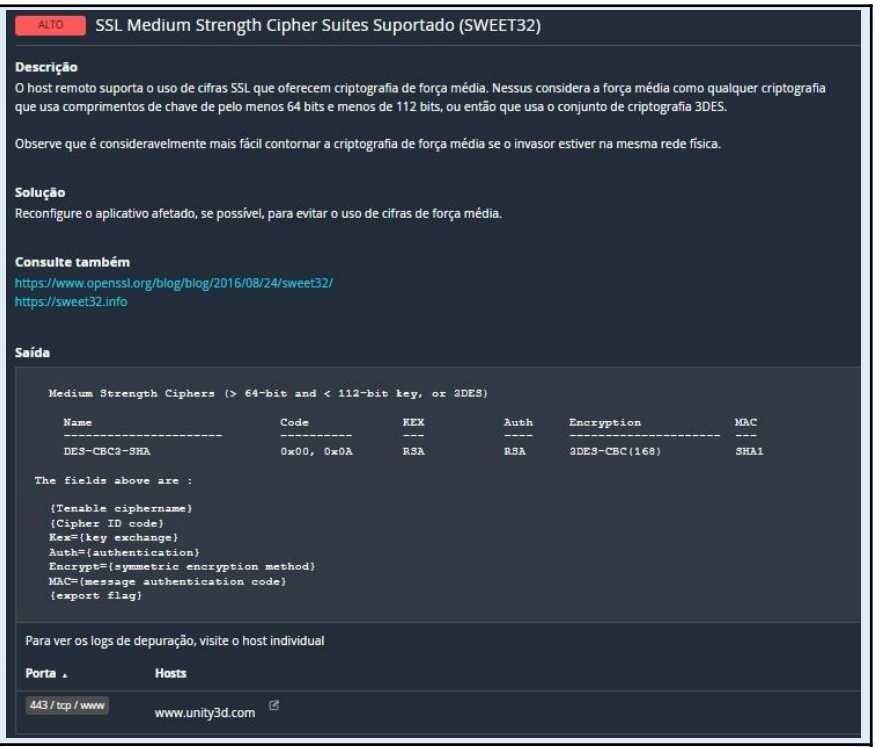
8 VULNERABILIDADES ENCONTRADAS

ID da Vulnerabilidade 1	
Criticidade	Média
Título	HSTS ausente do servidor HTTPS (RFC 6797)
Descrição	O servidor Web remoto não está impondo o HSTS, conforme definido pela RFC 6797. O HSTS é um cabeçalho de resposta opcional que pode ser configurado no servidor para instruir o navegador a se comunicar apenas via HTTPS. A falta de HSTS permite ataques de downgrade, ataques man-in-the-middle que removem SSL e enfraquece as proteções de sequestro de cookies.
URL afetado	www.unity3d.com
Evidência	
Recomendação	Configure o servidor Web remoto para usar o HSTS.

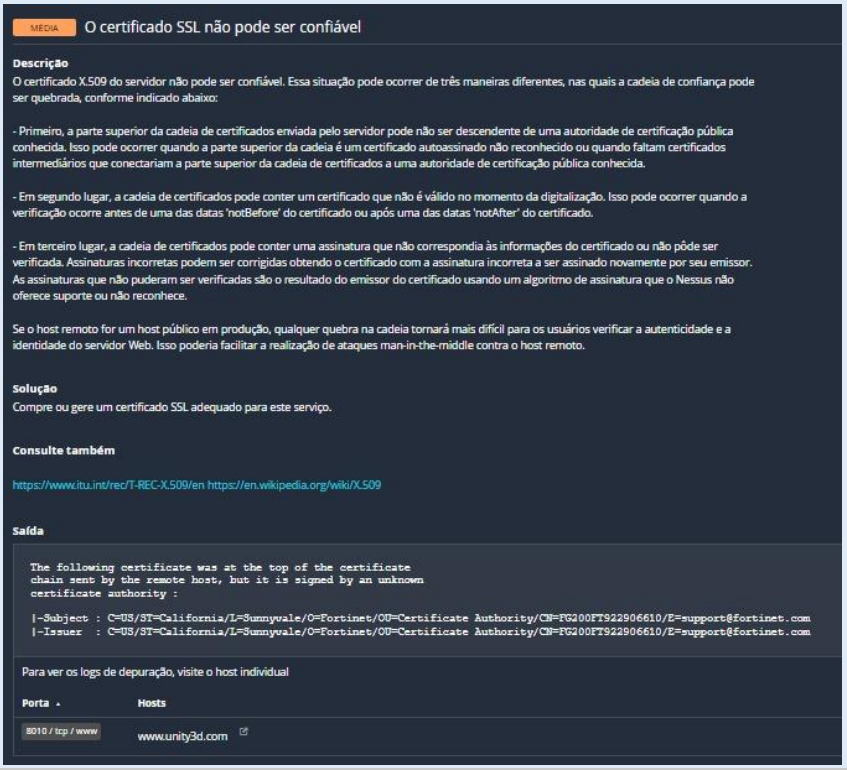
ID da Vulnerabilidade 2	
Criticidade	Informativa
Título	SSL Perfect Forward Secrecy Cipher Suites Suportado
Descrição	O host remoto suporta o uso de cifras SSL que oferecem criptografia PFS (Perfect Forward Secrecy). Esses conjuntos de codificação garantem que o tráfego SSL registrado não possa ser quebrado em uma data futura se a chave privada do servidor estiver comprometida.
URL afetado	www.unity3d.com

Evidência	
Recomendação	

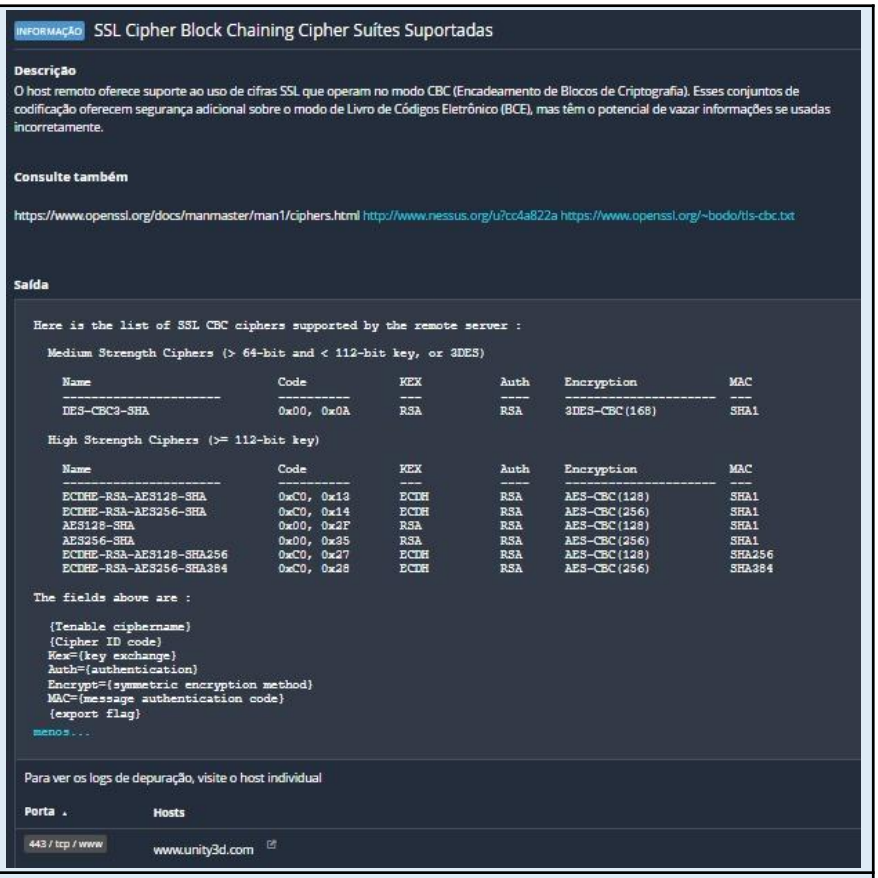
ID da Vulnerabilidade 3	
Criticidade	Alta
Título	SSL Medium Strength Cipher Suites Suportado (SWEET32)
Descrição	O host remoto suporta o uso de cifras SSL que oferecem criptografia de força média. Nessus considera a força média como qualquer criptografia que usa comprimentos de chave de pelo menos 64 bits e menos de 112 bits, ou então que usa o conjunto de criptografia 3DES.
URL afetado	www.unity3d.com

Evidência	
Recomendação	Reconfigure o aplicativo afetado, se possível, para evitar o uso de cifras de força média..

ID da Vulnerabilidade 4	
Criticidade	Média
Título	O certificado SSL não pode ser confiável
Descrição	O certificado X.509 do servidor não pode ser confiável. Essa situação pode ocorrer de três maneiras diferentes, nas quais a cadeia de confiança pode ser quebrada, conforme indicado abaixo: - Primeiro, a parte superior da cadeia de certificados enviada pelo servidor pode não ser descendente de uma autoridade de certificação pública conhecida. Isso pode ocorrer quando a parte superior da cadeia é um certificado autoassinado não reconhecido ou quando faltam certificados intermediários que conectariam a parte superior da cadeia de certificados a uma autoridade de certificação pública conhecida. - Em segundo lugar, a cadeia de certificados pode conter um certificado que não é válido no momento da digitalização. Isso pode ocorrer quando a verificação ocorre antes de uma das datas 'notBefore' do certificado ou após uma das datas 'notAfter' do certificado. - Em terceiro lugar, a cadeia de certificados pode conter uma assinatura que não correspondia às informações do certificado ou não pôde ser verificada. Assinaturas incorretas podem ser corrigidas obtendo o certificado com a assinatura incorreta a ser assinado novamente por seu emissor. As assinaturas que não puderam ser verificadas são o resultado do emissor do certificado usando um algoritmo de assinatura que o Nessus não oferece suporte ou não reconhece.

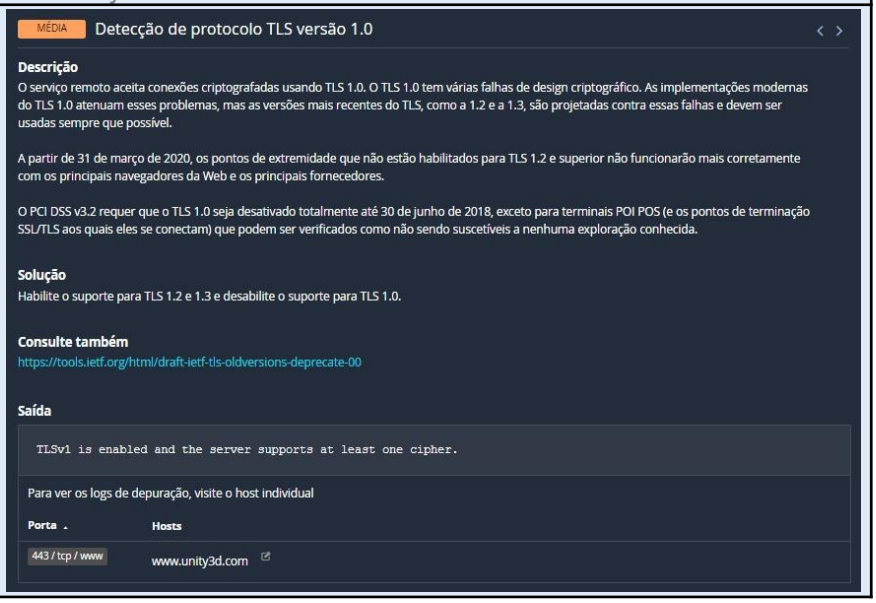
	Se o host remoto for um host público em produção, qualquer quebra na cadeia tornará mais difícil para os usuários verificar a autenticidade e a identidade do servidor Web. Isso poderia facilitar a realização de ataques man-in-the-middle contra o host remoto.
URL afetado	www.unity3d.com
Evidência	
Recomendação	Compre ou gere um certificado SSL adequado para este serviço.

ID da Vulnerabilidade 5	
Criticidade	Informativa
Título	SSL Cipher Block Chaining Cipher Suítes Suportadas
Descrição	O host remoto oferece suporte ao uso de cifras SSL que operam no modo CBC (Encadeamento de Blocos de Criptografia). Esses conjuntos de codificação oferecem segurança adicional sobre o modo de Livro de Códigos Eletrônico (BCE), mas têm o potencial de vazar informações se usadas incorretamente.
URL afetado	www.unity3d.com

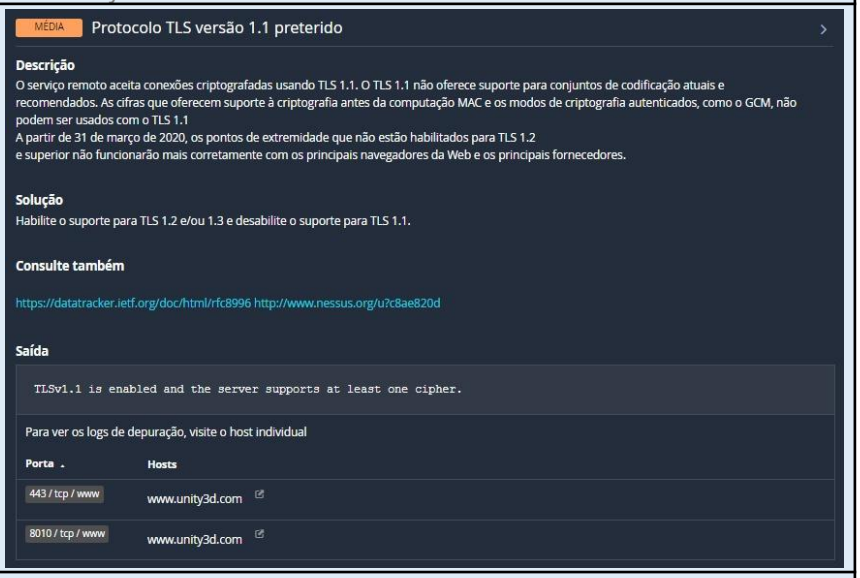
Evidência	
Recomendação	

ID da Vulnerabilidade 6	
Criticidade	Média
Título	Certificado autoassinado SSL
Descrição	A cadeia de certificados X.509 para este serviço não é assinada por uma autoridade de certificação reconhecida. Se o host remoto for um host público em produção, isso anulará o uso de SSL, pois qualquer pessoa poderá estabelecer um ataque man-in-the-middle contra o host remoto. Observe que esse plug-in não verifica se há cadeias de certificados que terminam em um certificado que não é autoassinado, mas é assinado por uma autoridade de certificação não reconhecida.
URL afetado	www.unity3d.com

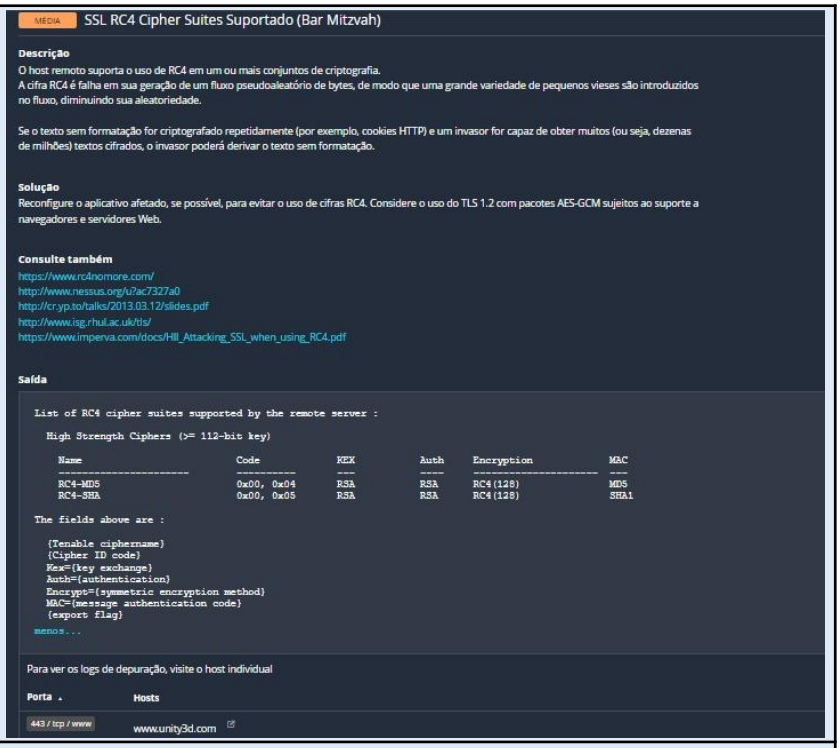
Evidência	
Recomendação	Compre ou gere um certificado SSL adequado para este serviço.

ID da Vulnerabilidade 7	
Criticidade	Média
Título	Detecção de protocolo TLS versão 1.0
Descrição	O serviço remoto aceita conexões criptografadas usando TLS 1.0. O TLS 1.0 tem várias falhas de design criptográfico. As implementações modernas do TLS 1.0 atenuam esses problemas, mas as versões mais recentes do TLS, como a 1.2 e a 1.3, são projetadas contra essas falhas e devem ser usadas sempre que possível. A partir de 31 de março de 2020, os pontos de extremidade que não estão habilitados para TLS 1.2 e superior não funcionarão mais corretamente com os principais navegadores da Web e os principais fornecedores. O PCI DSS v3.2 requer que o TLS 1.0 seja desativado totalmente até 30 de junho de 2018, exceto para terminais POI POS (e os pontos de terminação SSL/TLS aos quais eles se conectam) que podem ser verificados como não sendo suscetíveis a nenhuma exploração conhecida.
URL afetado	www.unity3d.com
Evidência	

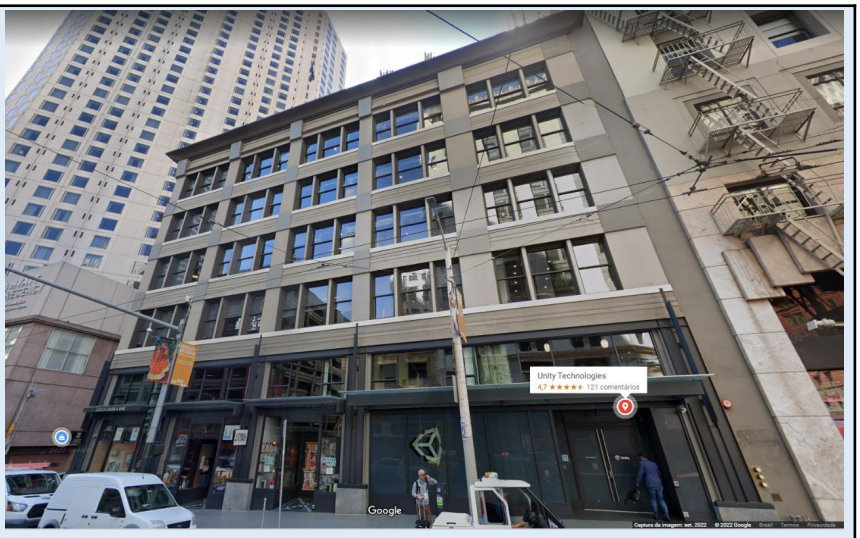
Recomendação	Habilite o suporte para TLS 1.2 e 1.3 e desabilite o suporte para TLS 1.0.

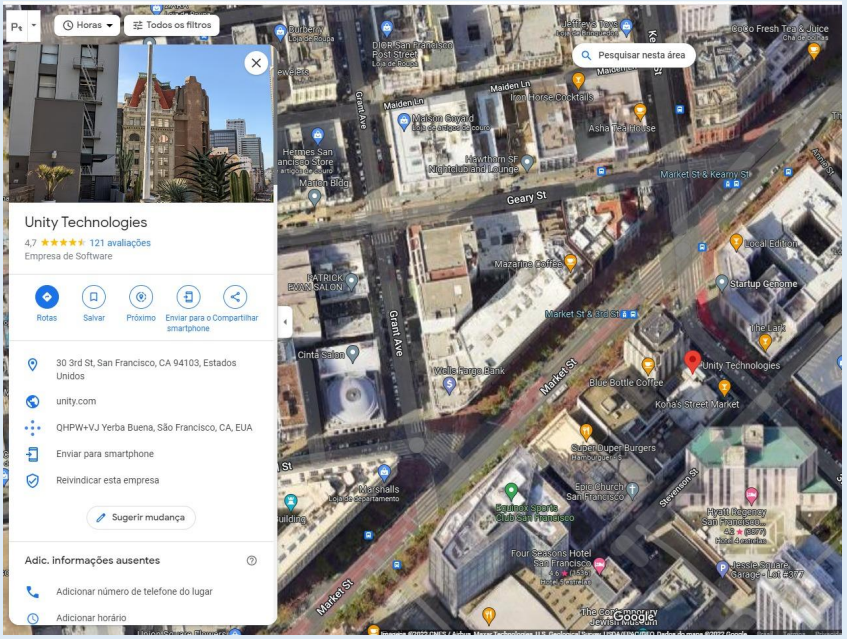
ID da Vulnerabilidade 8	
Criticidade	Média
Título	Protocolo TLS versão 1.1 preterido
Descrição	O serviço remoto aceita conexões criptografadas usando TLS 1.1. O TLS 1.1 não oferece suporte para conjuntos de codificação atuais e recomendados. As cifras que oferecem suporte à criptografia antes da computação MAC e os modos de criptografia autenticados, como o GCM, não podem ser usados com o TLS 1.1 A partir de 31 de março de 2020, os pontos de extremidade que não estão habilitados para TLS 1.2 e superior não funcionarão mais corretamente com os principais navegadores da Web e os principais fornecedores.
URL afetado	www.unity3d.com
Evidência	
Recomendação	Habilite o suporte para TLS 1.2 e/ou 1.3 e desabilite o suporte para TLS 1.1.

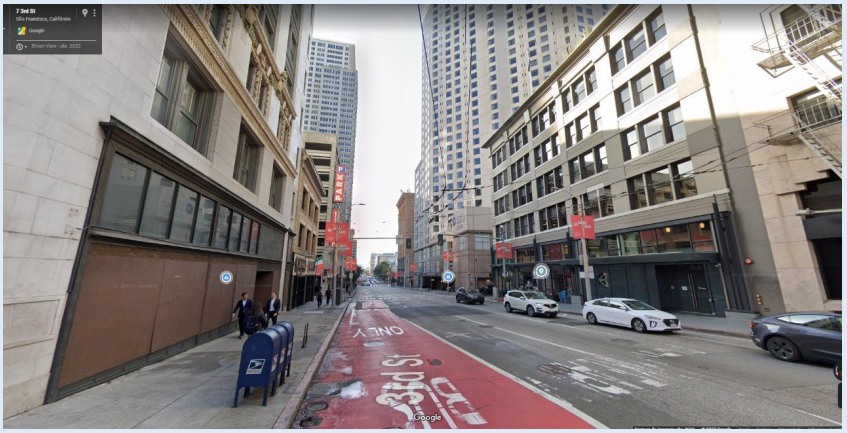
ID da Vulnerabilidade 9	
Criticidade	Média
Título	SSL RC4 Cipher Suites Suportado (Bar Mitzvah)
Descrição	O host remoto suporta o uso de RC4 em um ou mais conjuntos de criptografia. A cifra RC4 é falha em sua geração de um fluxo pseudo aleatório de bytes, de modo que uma grande variedade de pequenos vieses são introduzidos no fluxo, diminuindo sua aleatoriedade. Se o texto sem formatação for criptografado repetidamente (por exemplo, cookies HTTP) e um invasor for capaz de obter muitos (ou seja, dezenas de milhões) textos cifrados, o invasor poderá derivar o texto sem formatação.
URL afetado	www.unity3d.com

Evidência	
Recomendação	Reconfigure o aplicativo afetado, se possível, para evitar o uso de cifras RC4. Considere o uso do TLS 1.2 com pacotes AES-GCM sujeitos ao suporte a navegadores e servidores Web.

ID da Vulnerabilidade 10	
Criticidade	Informativa
Título	Vulnerabilidade via Google Maps (street)
Descrição	O endereço da sede da empresa demonstra que está localizado em ambiente comercial. Mas, logo ao lado e em frente tem bares, Restaurantes, cafeterias etc. que demonstram serem ótimos locais para encontros casuais de colegas de trabalho após o expediente. Ambientes propícios para que os funcionários estejam “desprotegidos” para dar informações por meio de técnicas de Engenharia Social.
Evidência	

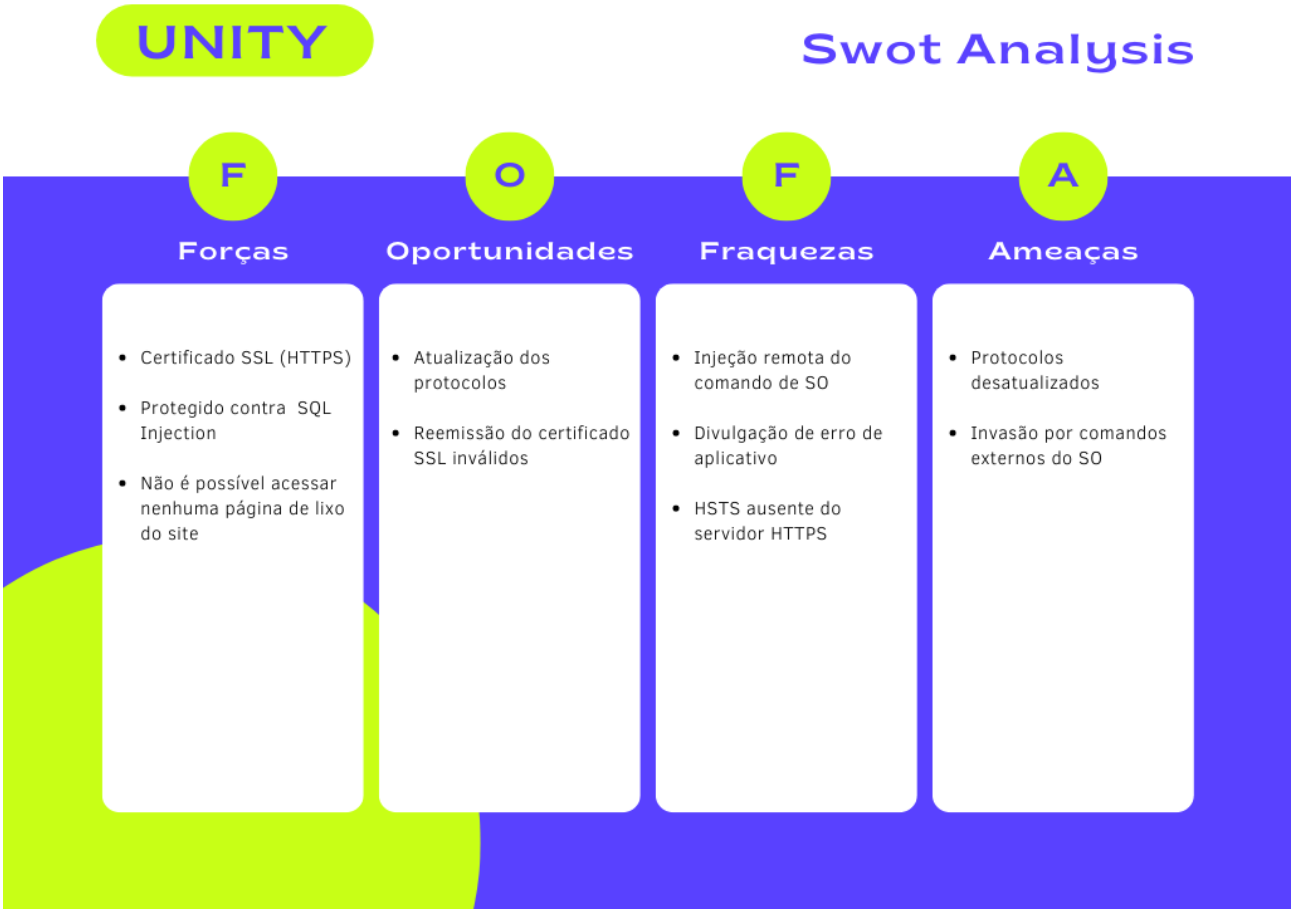






Recomendação	Criar uma cultura de preservação da identidade e ambiente empresarial. Ter política de segurança da informação bem cultivada dentro e fora da empresa. Promover treinamentos para evitar os riscos de um ataque causados por brechas humanas; trabalhar temas como de “O que é Engenharia social?” “Como evitar cryptojacking” E outros temas de segurança.

9 QUADRO SWOT DA SEGURANÇA DO SITE



10 TERMO DE PAGAMENTO

Condições		
Descrição	Valor/hora – R$ 128,03	Período 18 Dias
	Hora	Valor
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo	30 Horas	R$ 3.840,9
Provas de conceito e conclusão dos testes.	12 horas	R$ 1.536,36
Avaliação de riscos e esboço do relatório.	8 horas	R$ 1.024,24
Conclusão e revisão final do relatório	8 horas	R$ 1.024,24
Valor total		R$ 7.425,74

12 CONCLUSÕES E RECOMENDAÇÕES GERAIS

Conforme detalhado no item 6, e de acordo com as vulnerabilidades encontradas nos testes, é possível concluir que o sucesso de um ataque pode resultar em perdas financeiras, de ativos ou de recursos, além de causar danos à imagem da plataforma. Portanto, sua remediação é média para os negócios,

exigindo que seja providenciada em curto intervalo de tempo.

A abordagem dos testes realizados não considera a probabilidade do agente de ameaça, nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real sobre o negócio. É necessário que a área específica de segurança da plataforma defina qual o grau de risco de segurança das aplicações que está disposta a aceitar.

Cabe ressaltar, que novas ameaças, novas vulnerabilidades e mudanças na probabilidade ou nas consequências podem vir a ampliar os riscos anteriormente avaliados como pequenos. Convém que a análise crítica dos riscos pequenos e aceitos considere cada risco separadamente e em conjunto, a fim de avaliar seu impacto potencial agregado. Se os riscos não estiverem dentro da categoria "informativo" ou "baixo", convém que eles sejam tratados utilizando-se uma ou mais de uma das opções consideradas.

13 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27005:2011: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro: 2011

FIRST. **Common Vulnerability Scoring System v3.1**. 2019. Disponível em: https://www.first.org/cvss/ . Acesso em novembro de 2021

LAB, Access Security. **Relatório de Análise de Vulnerabilidades e Testes de Intrusão** Disponível em: <https://anubis.website/docs/report_access_pentest_anbistrade.pdf> Acesso em novembro de 2022.

EMPRESARIAS, Soluções. **TERMO ESPECÍFICO DO PRODUTO – VAMPS**. Disponível em: <https://www.vivo.com.br/content/dam/vivo-sites/vivo-com-br/pdf/para-empresas/regulatorio/solucoes-digitais/termo-especifico-vamps.pdf>. Acesso em novembro 2022

Anexo I

DECLARAÇÃO DE AUTORIZAÇÃO DO CONTRATANTE

INSTRUMENTO PARTICULAR DE PRESTAÇÃO DE SERVIÇOS DE TESTE DE INTRUSÃO (PENTEST)

CONTRATADA: **BRIAN SAMUEL DE SOUZA DANTAS e LEANDRO ROCHA DE CARVALHO**, estabelecida **NA RODOVIA BR 101, KM 197, CAPOEIRUÇU, CACHOEIRA - BA**, inscrita no CNPJ sob **nº 07.114.699/0001-60**, neste ato representada pelo Sr., brasileiro**, BRIAN SAMUEL DE SOUZA DANTAS**, Portador do RG **nº 22.125.542-1** e inscrito no CPF sob **nº 864.673.905-80**.

CONTRATANTE: **Unity Technologies**, estabelecida **NA RUA Broadway 21, CA 94133 San Francisco, Estados Unidos**, inscrita no CNPJ sob **nº 35.240.232/0001-00,** neste ato representada pelo Sr., suíço, **PIETRO SUPINO**, portador do RG **nº 16.532.690-6,** e inscrito no CPF sob **nº 904.077.200-22.**

As partes acima identificadas têm, entre si, justo e acertado o presente Contrato de Prestação de Serviços de Teste de Intrusão (Pentest), que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

1) DO OBJETO

O presente contrato tem por objeto, a realização de Teste de Intrusão (Pentest), a ser realizado pela CONTRATADA junto à CONTRATANTE, sendo que referidos testes somente poderão ser realizados nos dias e horários acordados, discriminados na Cláusula 2ª.

A CONTRATADA conduzirá um PENETRATION TESTING contra e-commerce/rede/sistema Unity.

Tais testes, consistem em simulações de ataques reais, resultando na descoberta de falhas da configuração e/ou vulnerabilidades. Vulnerabilidades estas que possam vir a permitir que a CONTRATANTE sofra impactos com ataques direcionados, perdendo a disponibilidade, integridade e confidencialidade de informações e sistemas.

2) DA EXECUÇÃO DOS SERVIÇOS

2.1 Escopo

O PENETRATION TESTING escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

O trabalho deve ser executado no seguinte escopo:

https://unity.com/

A CONTRATADA tem permissão de explorar o Escopo em sua Integralidade

2.2 Limitações do Escopo

A CONTRATANTE determina as seguintes limitações à realização dos referidos testes:

Negação de serviço, Problemas de limitação de taxa, Spamming, Falsificação de e-mail, Engenharia social (incluindo phishing) de funcionários ou contratados da Unity, Quaisquer tentativas físicas contra propriedades ou data centers da Unity, Auto-XSS e problemas exploráveis apenas por auto-XSS, problemas relacionados ao window.opener, Problemas de segurança de cookies para cookies sem sessão, Segurança do cabeçalho HTTP, Questões profundas de defesa, Entrar/Sair CSRF, Relatórios automatizados de ferramentas, Presença de preenchimento automático em formulários da web, Ataques exploráveis apenas em navegadores mais antigos ou navegadores com configurações não padrão, Redirecionamentos abertos (a menos que possam ser usados para roubar tokens ativamente), Relatórios informando que o software está desatualizado ou vulnerável sem uma

prova de conceito, Preocupações com as melhores práticas sem uma demonstração de explorabilidade prática, Formulários de contato e suporte , Injeção de HTML que não leva a XSS. (HTTPS://OWASP.ORG/WWW-PROJECT-SECURE-HEADERS/), POR EXEMPLO.

2.3 JANELA DE TESTES

Referidos testes, deverão ser realizados dentro do horário comercial, ou seja, de segunda à sexta-feira das 09:00 às 18 :00 horas.

Todas as fases do teste poderão ser acompanhadas e supervisionadas à critério da CONTRATANTE. Caso opte pelo acompanhamento, tal supervisão somente poderá ser realizada pelo responsável indicado e qualificado pela CONTRATANTE na Cláusula 3ª.

O teste de invasão deverá obedecer às seguintes fases:

1 Planejamento;

2 Descoberta;

3 Ataque (exploração);

4. Relatório de recomendações

5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

6. Reavaliação, novo teste pós remediação

7. Relatório final pós remediação

3) DAS RESPONSABILIDADES

A responsabilidade da CONTRATADA restringe-se apenas detectar e apontar os riscos existentes com relação à integridade e vulnerabilidade dos sistemas da CONTRATANTE e tão somente, apresentar formas para minimizá-los.

O trabalho desenvolvido pela CONTRATADA não tem como objetivo corrigir as possíveis vulnerabilidades, tampouco, proteger a CONTRATANTE contra-ataques internos e externos.

As recomendações feitas pela CONTRATADA devem ser validadas antes de serem colocadas em produção, a CONTRATADA não se responsabilizará por erros de implementações.

Será de responsabilidade da CONTRATANTE, garantir a segurança ao acesso dos relatórios entregues pela CONTRATADA, bem como a indicação dos responsáveis pelo acompanhamento da realização dos referidos testes, conforme disposto no competente TERMO DE ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÕES em sua cláusula 4ª, item 4.2, anexo a este instrumento, sendo a pessoa indicada pela CONTRATANTE, devidamente qualificada abaixo:

Responsável nomeado pela CONTRATANTE:

Nome: JOHN RICCITIELLO

CPF: nº 512.649.259-13

RG: nº 16.532.690-6

TELEFONE: (49) 2911-2287

E-MAIL: unity@unityseven.com.br

CIENTE: BRIAN SAMUEL DE SOUZA DANTAS e LEANDRO ROCHA DE CARVALHO

4) DO PRAZO CONTRATUAL

O presente contrato terá validade única e exclusivamente durante o período de realização da atividade contratada, ou seja, 40 (quarenta) horas testes, a partir da data da assinatura do presente contrato, podendo ser prorrogado por comum acordo entre as partes até a conclusão dos serviços contratados.

O presente contrato poderá ser rescindido ocorrendo pelo menos uma das seguintes situações:

a) por mútuo consentimento;

b) por qualquer das partes, mediante manifestação por escrito com antecedência mínima de 30 (trinta) dias, se a outra parte descumprir quaisquer obrigações assumidas no presente Contrato.

Fica estipulada a multa de 20% (vinte por cento), sobre o valor contratual, na qual incorrerá a parte que infringir qualquer uma das cláusulas deste contrato, ressalvada à parte inocente o direito de poder considerar simultaneamente rescindido o presente contrato, independentemente de qualquer outra formalidade judicial ou extrajudicial. A multa será sempre paga integralmente, seja qual for o prazo decorrido do presente contrato, ficando claro que o pagamento dessa multa não exime o pagamento de outras despesas inerentes ao contrato.

5) DO PAGAMENTO

Em contrapartida aos serviços contratados, a CONTRATANTE pagará à CONTRATADA, o valor **de R$ 1966,80 (MIL, NOVECENTOS E SESSENTA E SEIS REAIS E OITENTA CENTAVOS)** por **72 Horas** de serviços prestados, que serão pagos da seguinte forma:
A não efetivação do pagamento na forma e prazo pactuados acima, por culpa da CONTRATANTE fica estipulada a multa de 10% (dez por cento), juros moratórios à razão de 1% (um por cento) ao mês e correção monetária, além de outras despesas decorrentes de cobrança judicial ou extrajudicial.

6) DA AUTORIZAÇÃO

Para que seja alcançado o objetivo da atividade contratada e, para que esta possa ser realizada em sua integralidade, a CONTRATANTE, neste

ato, AUTORIZA a CONTRATADA, a realizar o Teste de Intrusão (pentest), objeto do presente contrato, devendo-se sempre, ambas as partes, assegurar a segurança das informações obtidas e fornecidas, bem como, cumprirem com seus deveres de confidencialidade de informações, devidamente pactuado entre as partes, conforme TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES, parte integrante do presente contrato.

7) DAS CONDIÇÕES GERAIS

Este Contrato constitui o único documento que regula os direitos e obrigações das partes, com relação aos serviços contratados, ficando expressamente cancelado ou revogado, todo e qualquer entendimento ou ajuste porventura existente que não esteja explicitamente consignado neste Contrato.

Caso as partes envolvidas deixem de exigir em qualquer tempo o cumprimento de quaisquer cláusulas ou condições deste contrato, a parte prejudicada não ficará impedida de, quando o entender, fazer com que a parte inadimplente cumpra rigorosamente todas as condições contratuais.

Caso a CONTRATADA admitir em benefício do CONTRATANTE qualquer atraso no pagamento das mensalidades ou no cumprimento de qualquer outra obrigação contratual, essa tolerância não poderá ser considerada como alteração das condições deste contrato, pois se constituirá em ato de mera liberdade da CONTRATADA.

As partes contratantes elegem o foro da comarca de São Paulo, cujo foro é o único competente, com renúncia expressa de qualquer outro por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução do presente Contrato.

E, por estarem justos e contratados, cientes e de acordo com todas as cláusulas e condições do presente Contrato de Prestação de Serviços de Teste de Intrusão (Pentesters), assinam este instrumento em duas vias para um só efeito na presença das testemunhas abaixo.

Cachoeira-BA, 02 de Dezembro de 2022

BRIAN SAMUEL DE SOUZA DANTAS
LEANDRO ROCHA DE CARVALHO **JOHN RICCITIELLO**

CONTRATADA CONTRATANTE

TESTEMUNHAS:

Nome: _____

CPF: _____

Nome: _____

CPF: _____