UTILIZAÇÃO DOS PROTOCOLOS TLS 1.0 E 1.1

Coordenação de Engenharia de Software
Segurança da Informação

Belo Horizonte, outubro de 2020

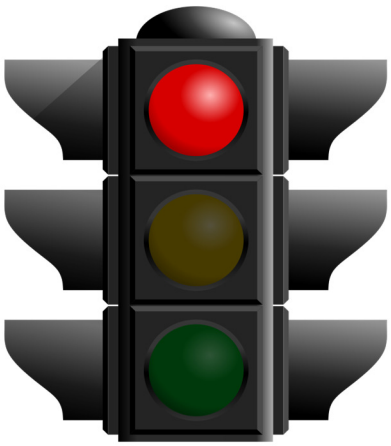
TERMO DE CONFIDENCIALIDADE

Este documento contém informações confidenciais e sensíveis referente à segurança do ambiente operacional da UNIMED-BH, sendo de extrema importância seu sigilo, protegido conforme políticas de segurança da corporação que se destina.

Esse documento, ou as informações nele contido, não podem ser usados, copiados, divulgados ou encaminhados sem autorização prévia da UNIMED-BH.

SUMÁRIO

SUMÁRIO EXECUTIVO



Vulnerabilidades críticas, que comprometem a aplicação/app e o ambiente de produção. Não deve ser implantado sem correção.

Vulnerabilidades intermediárias. Podem comprometer a aplicação/app e o ambiente de produção. Fortemente recomendada a correção. De acordo com o grau da vulnerabilidade, pode ser impeditivo ou não sua implantação.

Vulnerabilidades baixas, recomendadas correções. Não é impeditivo para implantação.

A manutenção do suporte às versões 1.0 e 1.1 do protocolo de criptografia TLS expõe o ambiente da cooperativa a riscos, visto que existem diversas vulnerabilidades documentadas, inclusive com *exploites*, que podem ser utilizadas para acesso indevido às informações trocadas entre os sistemas web da Unimed-BH e seus clientes e/ou prestadores.

Além disso, os principais navegadores do mercado deixaram de suportar essas versões do protocolo, passando a exibir um alerta para o usuário quando este tenta acessar um domínio que ainda suporta essas versões.

É de extrema importância que todas as aplicações de responsabilidade da Unimed-BH, assim como todos os serviços disponibilizados pela mesma, deixem de suportar essas versões desatualizadas o mais rápido possível.

Sinal	VULNERABILIDADES
🔴	Manutenção do suporte das versões 1.0 e 1.1 do protocolo TLS

1. LINHAS GERAIS

1.1. Introdução

Os principais navegadores do mercado deixaram de suportar as versões 1.0 e 1.1 do protocolo TLS utilizado para criptografar as informações trafegadas entre um sistema e os navegadores dos clientes ou entre dois sistemas.
Essa alteração deveria ter sido aplicada já no início de 2020 mas devido à pandemia do Covid 19 foi postergado até mais ou menos o meio desse ano, quando foi aplicado ao Chrome, Edge, Firefox e aos demais navegadores mais utilizados mundialmente.

1.2. Objetivo e Escopo da Análise

Este relatório tem como objetivo apresentar os riscos da manutenção do suporte de versões antigas do protocolo de criptografia TLS no ambiente web da Unimed-BH.

1.3. Fundamentação

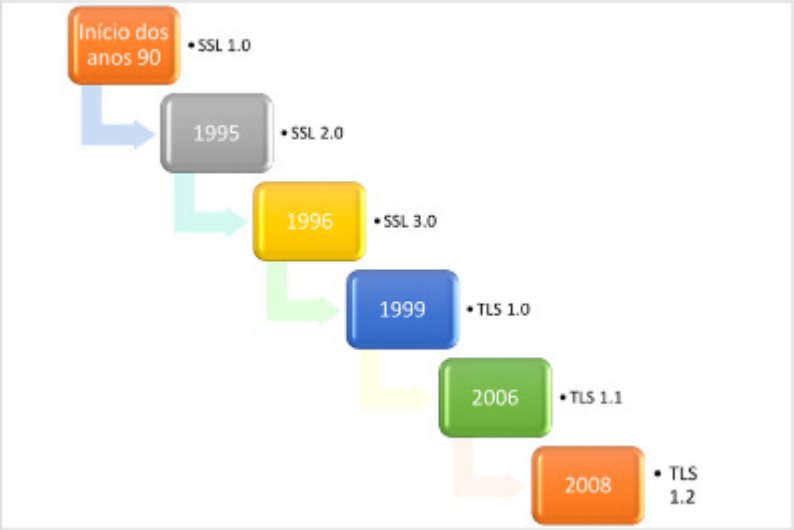
A elaboração deste documento fundamenta-se no Procedimento Gerencial **PL.GGC.GGRC.013 – Segurança da Informação e Sigilo**, que visa garantir os princípios de integridade, confidencialidade, disponibilidade, autenticidade e legalidade; **Procedimento Gerencial PG.GSI.GGTI.016 – Desenvolvimento Seguro de Sistemas de TI** que tem como objetivo estabelecer as determinações e as responsabilidades para o desenvolvimento seguro de sistemas de TI, a fim de tornar o processo de concepção, desenvolvimento e manutenção de sistemas para a Unimed-BH mais confiável, aditável, estável e protegido contra ameaças, durante todo o ciclo de vida do aplicativo; conformidade com a **ISO/EIC 27002** que objetiva a determinação de diretrizes e princípios gerais para iniciar, manter e melhorar a gestão de segurança da informação, englobando a implantação e gerenciamento de controles, levando em conta os ambientes de risco encontrados na organização.

2. ANÁLISE DA PROBLEMA

A Unimed-BH, visando estar em conformidade com as melhores práticas de segurança da informação, recomenda desabilitar o suporte às versões 1.0 e 1.1 do protocolo de criptografia TLS em seus sistemas de informação.

O TLS (*Transport Layer Security*) é um protocolo de criptografia usado para estabelecer um canal de comunicação seguro entre dois sistemas. É usado para autenticar um ou ambos os sistemas, e proteger a confidencialidade e a integridade da informação que trafega entre eles. Foi desenvolvido originalmente como *Secure Sockets Layer* (SSL) pela Netscape no início dos anos 90. Padronizado pelo *Internet Engineering Taskforce* (IETF), o TLS passou por várias revisões para melhorar a segurança para bloquear ataques conhecidos e adicionar suporte a novos algoritmos de criptografia, com grandes revisões ao SSL 3.0 em 1996, TLS 1.0 em 1990, TLS 1.1 em 2006 e TLS 1.2 em 2008.

Abaixo segue uma figura que mostra a evolução das versões do SSL/TLS ao longo do tempo:



As versões 1.0 e 1.1 não são mais consideradas seguras para garantir a confidencialidade e a integridade das informações que estão sendo trafegadas. Além disso, os principais navegadores do mercado não estão mais suportando essas versões.

Vale lembrar que independentemente do navegador, o uso de protocolos antigos coloca o ambiente e seus usuários na mira de cibercriminosos. Existem diversas vulnerabilidades graves nas versões antigas do TLS que se não tratadas deixam as informações da cooperativa em sério risco de exposição indevida.

De acordo com o NIST (*National Institute of Standards and Technology*), não existe nenhuma maneira que possa reparar as versões antigas do TLS. Assim sendo, é de crítica importância que as organizações façam a migração para uma alternativa segura o mais rápido possível, e desabilite qualquer comunicação utilizando versões antigas do TLS.

2.1. Vulnerabilidade a ataques

A seguir vamos descrever de forma sucinta os principais ataques que podem ser utilizados para explorar as vulnerabilidades existentes nas versões do protocolo TLS1.1 e seus antecessores:

- **Heartbleed attack;**

Este tipo de ataque permite roubar informação protegida, tais como credenciais de acesso, por exemplo. Compromete as chaves privadas usadas para encriptar a comunicação, sendo possível ter acesso às informações trafegadas.

- **Length extension attack;**

Este tipo de ataque acontece quando certos tipos hash são usados indevidamente como MAC, o que permite ao atacante adicionar informação extra à mensagem. Algoritmos criptográficos para o cálculo de hash baseados na construção de "*Merkle-Damgård*", tais como MD5, SHA-1 e SHA-2, por exemplo, estão vulneráveis a este ataque. Os algoritmos MD2, SHA-224, SHA-3 e SHA-384, por exemplo, não são vulneráveis a este ataque.

- **Man-in-the-middle attack (MITM)**

Este tipo de ataque permite ao atacante se inserir no meio de uma conexão e fazer-se passar por ambas as partes (cliente e servidor, por exemplo), onde toda a informação trocada é passada pelo atacante. Ao ter sucesso, o atacante pode manipular os dados trocados entre as partes envolvidas.

- **BEAST attack**

O ataque *Browser Exploit Against* SSL/TLS (BEAST), afeta as versões anteriores do protocolo TLS1.0 (inclusive). Este ataque aproveita as vulnerabilidades do CBC, que juntamente com o ataque MITM conseguem desencriptar e obter os *authentication tokens*, dando acesso aos dados transmitidos entre o servidor e o navegador do cliente.

- **POODLE attack**

O ataque *Padding Oracle On Downgraded Legacy Encryption* –POODLE é um pouco semelhante ao ataque BEAST. Também aproveita as fragilidades do CBC, que juntamente com o ataque MITM, permitem desencriptar informação numa comunicação com o protocolo SSL3.0.

3. RECOMENDAÇÕES DE SEGURANÇA

Frente as informações apresentadas, a equipe de Segurança da Informação recomenda veementemente que o suporte às versões 1.0 e 1.1 do protocolo TLS sejam descontinuados o mais rápido possível, passando assim a operar somente na versão 1.2 ou superior.

Também é recomendado que seja comunicado o mais rápido possível aos nossos prestadores e parceiros de negócios a necessidade de adequação das suas aplicações e sistemas para operar com TLS 1.2 ou 1.3 (Recomendamos a 1.3 por se tratar de uma versão mais nova que possui segurança e desempenho aprimorados), a fim de evitar que possíveis integrações entre estes sistemas e os da Unimed-BH deixem de funcionar quando desativarmos o suporte às versões antigas.


Unimed
Belo Horizonte