Cliente	**Liberado em**	**Emitido em**
TJAC	27/06/2024	27/06/2024 15:10:19
SISTEMA	**Versão**	**Itens acumulados de**
ESAJ-PERFIL	24.02.00-00	24.02.00-00

Alteração de Sistema (1)

SISTEMA e-SAJ

Chamado/SALT/Cliente/Contato		
Chamado: Não informado - Cliente: Equipe SAJ - Contato: Não informado		
Caminho (módulo/ domínio)	**Demanda**	**Causa**
Administração de Sistema	No cenário tecnológico em constante evolução em que vivemos, a segurança das aplicações é um dos temas prioritários, pois, à medida que novas vulnerabilidades e ameaças surgem, é necessário manter os sistemas atualizados e seguros. Este projeto tem por objetivo a atualização e elevação da segurança nas aplicações do ESAJPerfil, garantindo o funcionamento contínuo e confiável de nossas aplicações, mas também reduzindo o risco de exposição a vulnerabilidades conhecidas e potenciais ataques.	Este projeto tem por objetivo a atualização e elevação da segurança nas aplicações do ESAJPerfil, garantindo o funcionamento contínuo e confiável de nossas aplicações, mas também reduzindo o risco de exposição a vulnerabilidades conhecidas e potenciais ataques.
Local (categoria/ funcionalidade)	**Solução**	**Objetos Alterados**

Cliente	Liberado em	Emitido em
TJAC	27/06/2024	27/06/2024 15:10:19
SISTEMA	**Versão**	**Itens acumulados de**
ESAJ-PERFIL	24.02.00-00	24.02.00-00

Administração de Sistema do WEB	No mês de junho, foi finalizado o desenvolvimento para atualização dos Common Vulnerabilities and Exposures (CVEs), demais vulnerabilidades e vault na aplicação ESAJPerfil do Portal e-SAJ e será liberada na versão 24.02. 00-00. Seguem as atualizações realizadas: Sequestro de cookie: Foram implementadas medidas de segurança para proteger os cookies dos usuários, tornando-os mais seguros contra esse tipo de ataque. Além disso, foram adicionadas as flags HttpOnly, que bloqueia qualquer execução javascript de terceiros no site, SameSite=Strict e Secure=true, aumentando ainda mais a segurança dos cookies e reduzindo significativamente o risco de sequestro de cookies. ClickJanking: Foram implementadas correções no código para garantir que a interface do usuário não possa ser manipulada por scripts maliciosos, tornando a interação mais segura para os usuários. Possibilitar a geração da imagem docker sem acesso à repositórios externos: Foi modificado o processo de geração da imagem Docker para que possa ser feito sem a necessidade de acessar repositórios externos, garantindo assim uma geração mais segura e independente. Imagem docker atualizada, no padrão non-root e com o menor número de CVEs: Foi atualizada a imagem Docker para a versão mais recente, garantindo que ela esteja livre de vulnerabilidades conhecidas e configurada no padrão non-root, o que reduz os riscos de segurança. Suporte ao VAULT: Foi implementado o suporte ao VAULT, permitindo que a aplicação armazene e gerencie de forma segura seus segredos e chaves, melhorando assim a segurança geral do sistema. Remoção de informações sensíveis do info.do: Foram removidas as informações sensíveis do arquivo info. do, garantindo que não haja vazamento de dados confidenciais e protegendo assim a segurança da aplicação. Vulnerabilidades conhecidas: CORS: Foram implementadas medidas de segurança para mitigar os riscos de CORS, garantindo que apenas sites autorizados possam acessar os recursos da aplicação, protegendo assim contra ataques maliciosos. Converte para Java 17 e CVE: Foi atualizada a aplicação para utilizar o Java 17, que é a versão mais recente e segura, além de corrigir quaisquer vulnerabilidades conhecidas (CVEs) que possam existir na versão anterior. Isso garante maior segurança e eficiência no desenvolvimento. Listas de CVEs resolvidos na aplicação: CVE-2011-4457,CVE-2012-0881,CVE-2012-5783,CVE-2013-4002,CVE-2013-5679,CVE-2013-5960,CVE-2013-6440,CVE-2014-0107,CVE-2014-0114,CVE-2014-3603,CVE-2014-3604,CVE-2015-1796,CVE-2016-1000031,CVE-2016-10228,CVE-2016-3092,CVE-201,-5007,CVE-2016-9879,CVE-2017-18640,CVE-2017-7536,CVE-2018-1000632,CVE-2018-10237,CVE-2018-11039,CVE-2018-11040,CVE-2018-11771,CVE-2018-11797,CVE-2018-1257,CVE-2018-1258,CVE-2018-1324	

Cliente	Liberado em	Emitido em
TJAC	27/06/2024	27/06/2024 15:10:19
SISTEMA	**Versão**	**Itens acumulados de**
ESAJ-PERFIL	24.02.00-00	24.02.00-00

Objetos Alterados

Informações para Instalação

- A atualização da versão deve ser realizada em horário especial, ou seja, não pode ser realizada no horário de expediente;
- Para a atualização da versão o sistema não deve estar sendo executado, portanto, nenhum usuário deve estar conectado ao banco de dados;
- Fazer um backup da base de dados antes de iniciar a atualização;
- É obrigatória a análise das informações e dos pré-requisitos contidos nos scripts, principalmente nos scripts de alteração de modelo de dados (-X.sql);
- Em caso de erro na execução de qualquer script, a atualização da versão deve ser interrompida e deve ser realizado contato imediato com o suporte da Softplan;
- Após a execução de qualquer script de alteração de modelo de dados (-X.sql), é necessário que os objetos sejam reativados, para isso, execute o comando "reativaObj";