Empresa divulga relatório alarmante sobre segurança de dispositivos

“Relatório sobre o Estado da Segurança de Sistemas Ciberfísicos (CPS): Setor de Saúde 2023” revela lacunas alarmantes na segurança de dispositivos médicos diretamente ligados aos cuidados de pacientes

A Claroty, empresa de proteção de sistemas ciberfísicos (CPS), lançou na conferência anual HIMSS24, um novo relatório que revela dados preocupantes sobre a segurança de dispositivos médicos conectados a redes de organizações de saúde, como hospitais e clínicas. O Relatório “*The State of CPS Security: Healthcare 2023*″ revelou que surpreendentes 63% das Vulnerabilidades Exploradas e Conhecidas (KEVs) rastreadas pela CISA estão nessas redes, e que 23% dos dispositivos médicos, incluindo dispositivos de imagem, dispositivos clínicos, de IoT e dispositivos cirúrgicos, possuem pelo menos uma dessas vulnerabilidade (KEV).

Na primeira edição do *“The State of CPS Security Report: Healthcare”*, que tem foco no setor de saúde, o grupo premiado de pesquisadores da Claroty, o Team82, examina como o desafio de colocar cada vez mais dispositivos médicos e sistemas de pacientes conectados online aumenta a exposição à onda crescente de ataques cibernéticos voltados à interrupção de operações hospitalares. O objetivo desta pesquisa é demonstrar a ampla conectividade de dispositivos médicos críticos – desde sistemas de imagem até bombas de infusão -, e descrever as implicações de sua exposição no ambiente digital. A superfície de vulnerabilidades e fraquezas nas implementações identificadas pelos pesquisadores do Team82 da Claroty muitas vezes representam uma ameaça direta aos pacientes, podendo resultar em impactos negativos em cada um dos casos analisados.

“A conectividade impulsionou grandes mudanças nas redes hospitalares, criando melhorias no atendimento ao paciente com médicos aptos a diagnosticar, prescrever e tratar remotamente com uma eficiência nunca vista antes”, destaca Amir Preminger, vice-presidente de pesquisa da Claroty. “No entanto, o aumento da conectividade requer uma arquitetura de rede adequada e uma compreensão da exposição aos ataques que ela introduz. As organizações de saúde e seus parceiros de segurança devem desenvolver políticas e estratégias, que enfatizem a necessidade de dispositivos e sistemas médicos

resilientes capazes de resistir a invasões. Isso inclui o acesso remoto seguro, priorização de gestão de riscos e implementação de segmentação".

"O relatório elaborado pelo Team82 da Claroty ressalta a vital importância da segurança das organizações de saúde. Estamos atentos ao fato de que estamos lidando com vidas humanas, o que demanda um comprometimento total. Em um mundo em constante transformação, os pacientes estão cada vez mais conscientes e exigirão hospitais que ofereçam proteção para os seus equipamentos médicos. Em breve, essa será uma demanda essencial na escolha por parte do paciente, sobre onde buscar tratamento médico", destaca Italo Calvano, vice-presidente da Claroty para a América Latina.

Principais descobertas:

- **Exposição em Redes:** 22% dos hospitais conectam tanto as redes de visitantes (responsáveis por disponibilizar acesso Wi-Fi a pacientes e visitantes), quanto as redes internas. Isso cria um vetor de ataque perigoso, pois um cibercriminoso pode rapidamente encontrar e direcionar ativos na Wi-Fi pública e usar esse acesso como ponte para as redes internas, onde estão localizados os dispositivos aplicados em cuidados aos pacientes. A pesquisa do Team82 da Claroty mostrou que chocantes 4% dos dispositivos cirúrgicos – ou seja, equipamentos críticos que, se falharem, podem impactar negativamente o cuidado do paciente -, se comunicam em redes de visitantes.
- **Sistemas Operacionais Sem Suporte ou no Fim da Vida Útil:** 14% dos dispositivos médicos conectados estão sendo executados em sistemas operacionais sem suporte ou no fim da vida útil. Dos dispositivos sem suporte, 32% são de imagem, incluindo sistemas de raios-X e ressonância magnética, que são vitais para o diagnóstico e tratamento prescritivo, e 7% são dispositivos cirúrgicos.
- **Alta Probabilidade de Exploração:** o relatório examinou dispositivos com altas pontuações no Sistema de Pontuação de Previsão de Exploração (EPSS), que representam a probabilidade de que uma vulnerabilidade de software seja explorada na natureza em uma escala de 0 a 100. A análise mostrou que 11% dos dispositivos de pacientes, como bombas de infusão, e 10% dos dispositivos cirúrgicos contêm vulnerabilidades com altas pontuações

no EPSS. Aprofundando-se, ao analisar dispositivos com sistemas operacionais sem suporte, 85% dos dispositivos cirúrgicos nessa categoria têm altas pontuações no EPSS.

- **Dispositivos Remotamente Acessíveis:** a pesquisa analisou quais dispositivos médicos são remotamente acessíveis e descobriu que aqueles com uma alta consequência de falha, incluindo desfibriladores, sistemas cirúrgicos robóticos e *gateways* de desfibriladores, estão entre esse grupo. A pesquisa também mostrou que 66% dos dispositivos de imagem, 54% dos dispositivos cirúrgicos e 40% dos dispositivos de pacientes são remotamente acessíveis.

Para acessar a lista completa de descobertas do Team82 da Claroty, análises detalhadas e medidas de segurança recomendadas em resposta às tendências de vulnerabilidades, faça o *download* do "Relatório sobre o Estado da Segurança de Sistemas Ciberfísicos (CPS): Área de Saúde 2023" *("The State of CPS Security Report: Healthcare 2023").*

Metodologia

O Relatório *"The State of CPS Security: Healthcare 2023"* é um retrato das tendências de cibersegurança na área de saúde, vulnerabilidades de dispositivos médicos e incidentes observados e analisados por cientistas de dados e o Team82 (equipe de pesquisadores com foco em ameaças) da Claroty. Informações e *insights* de fontes abertas e confiáveis, incluindo o Banco Nacional de Dados de Vulnerabilidades (NVD), a Agência de Segurança Cibernética e Infraestrutura (CISA), o Grupo de Trabalho do Conselho Coordenador do Setor de Saúde e outros, também foram utilizados para trazer um contexto valioso às descobertas da Claroty.

Agradecimentos

O autor principal deste relatório é Chen Fradkin, cientista de dados *full stack* na Claroty. Contribuições incluem: Ty Greenhalgh, principal da indústria de saúde; Yuval Halaban, líder

da equipe de riscos; Rotem Mesika, líder do grupo de ameaças e riscos; Nadav Erez, vice-presidente de dados; e Amir Preminger, vice-presidente de pesquisa. Agradecimentos especiais a todo o Team82 da Claroty e ao departamento de dados por fornecerem um suporte excepcional para vários aspectos deste relatório, e os esforços de pesquisa que o impulsionaram.

Sobre a Claroty

A Claroty capacita as organizações a proteger sistemas ciberfísicos em ambientes industriais, de saúde, negócios e do setor público: a Internet das Coisas (XIoT). A plataforma unificada da empresa se integra à infraestrutura existente dos clientes, para fornecer uma gama completa de controles para visibilidade, gerenciamento de riscos e vulnerabilidades, detecção de ameaças e acesso remoto seguro. Com o apoio das maiores empresas de investimento do mundo e fornecedores de automação industrial, Claroty é implementado por centenas de organizações em milhares de localidades em todo o mundo. A empresa está sediada na cidade de Nova York e presente na Europa, Ásia-Pacífico e América Latina. Para saber mais sobre a Claroty, por favor, acesse claroty.com.