Instituto de Computação

SBSeg24 São José dos Campos

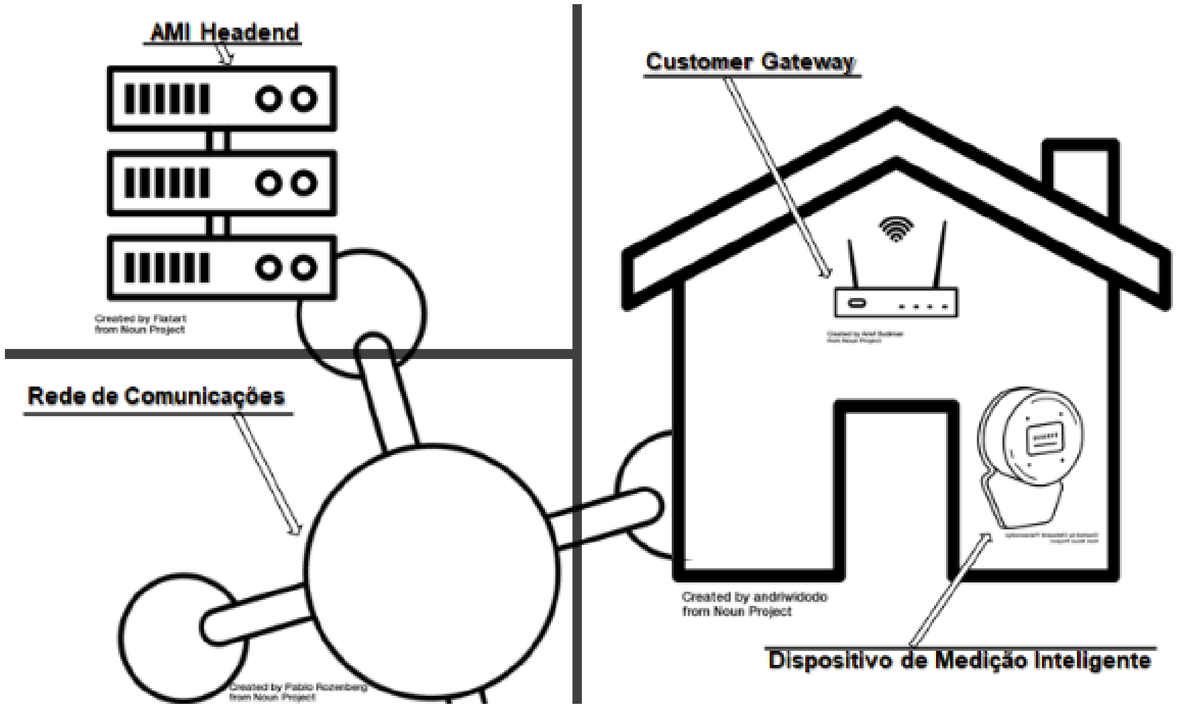
Realização: SBC Sociedade Brasileira de Computação

Vulnerabilidades de Segurança Cibernética em Dispositivos de Medição Avançada de Energia Elétrica

Bruno Macena dos Santos (1° autor)
Wesley H. Leite
Prof. Dr. Raphael C. S. Machado

Dispositivos de Medição Avançada - Contextualização

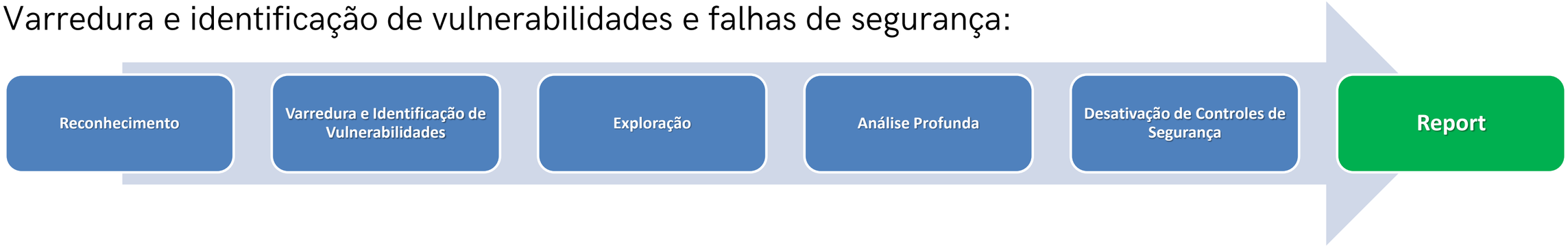
- São componentes essenciais nas redes de distribuição de Energia Elétrica;
- Registram e transmitem dados de consumo energético;
- Quando permitem a comunicação bidirecional entre o medidor e a concessionária de energia, são denominados de Medidores Inteligentes;
- Funcionam como elementos críticos e portas de entrada para as chamadas Infraestruturas de Medição Avançada (AMI).
- Estão inseridos no domínio de Internet das Coisas.



O objetivo deste trabalho é contribuir para a compreensão das fragilidades inerentes, identificando e classificando-as, avaliando a magnitude dos potenciais riscos à segurança cibernética da rede de distribuição de energia elétrica.

Metodologia

- Testes de intrusão (pentest) em dispositivos de medição avançada e na infraestrutura relacionada de AMI em condições operacionais reais
- Análise detalhada dos softwares embarcados.
- Reconhecimento da arquitetura, funcionalidades e os potenciais pontos de vulnerabilidade.
- Varredura e identificação de vulnerabilidades e falhas de segurança:



- Classificação das vulnerabilidades identificadas conforme a taxonomia do Common Weakness Enumeration (CWE)
- Pontuação de risco com base na metodologia Common Vulnerability Scoring System (CVS)
- Correlação com vulnerabilidades identificadas em padrões como OWASP IoT Top Ten.

Nota: Os resultados deste trabalho foram baseados em uma amostra selecionada de fabricantes e modelos de dispositivos, juntamente com suas plataformas de medição avançada relacionadas. Embora esta amostra pareça limitada à primeira vista, ela abrange uma parte significativa da base instalada e em operação no território nacional.

Resultados

Vulnerabilidades			Severidade	Medidor-001	Medidor-002	Medidor-003	Medidor-004	Medidor-005	Medidor-006
Categorização / Escopo	Controle de Acesso	CWE-521 CWE-1391	Médio	5.3					
		CWE-639	Alta	7.5	7.5	8.1			
		CWE-693			7.1		7.1		
		CWE-259						7.3	
		CWE-522		7.5	7.5			8.8	
	Outros	CWE-79							7.1

- Todos os medidores apresentam pelo menos uma vulnerabilidade considerada de alta severidade, com destaque para falhas no controle de acesso.
- A maioria dos impactos estava relacionada ao comprometimento da integridade dos dados de medição, o que poderia levar a manipulações e resultar em cobranças incorretas de consumo de energia.
- A exploração das vulnerabilidades exigia baixa complexidade e privilégios, aumentando a probabilidade de ocorrência de eventos cibernéticos relacionados.
- As vulnerabilidades já foram corrigidas pelos fabricantes.

Resultados – Exemplo

Credenciais insuficientemente protegidas : Acesso não autorizado

- CWE-522: Credenciais insuficientemente protegidas
- #3 do projeto TOP10 do OWASP Internet of Things

Métricas de Explorabilidade		Métricas de Impacto	
Vetor de Ataque (AV):	**Network/Rede (N)**	**Impacto na Confidencialidade (C):**	**High/Alto (H)**
Complexidade do Ataque (AC):	**Low/Baixo (L)**	**Impacto na Integridade (I):**	**High/Alto (H)**
Privilégios Necessários (PR):	**Low/Baixo (L)**	**Impacto na Disponibilidade (A):**	**High/Alto (H)**
Interação do Usuário (UI):	**None/Nenhum (N)**		
Escopo (S):	**Unchanged/Inalterado (U)**		
(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)		**CVSS Score: 8.8**	

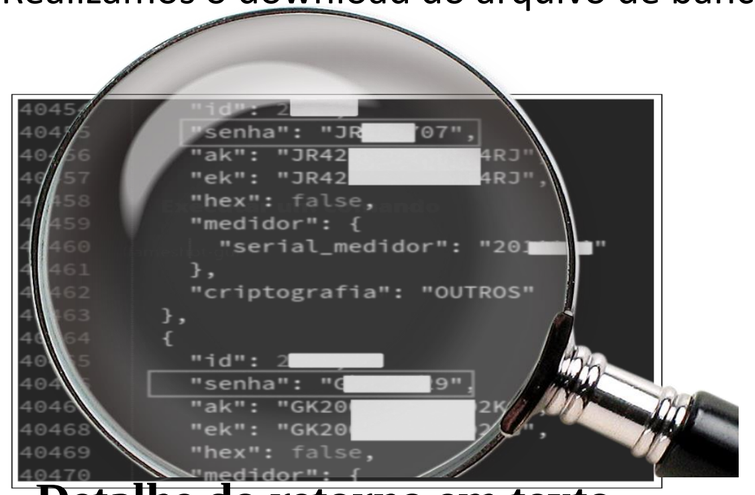
SEVERIDADE ALTA

OWASP IOT

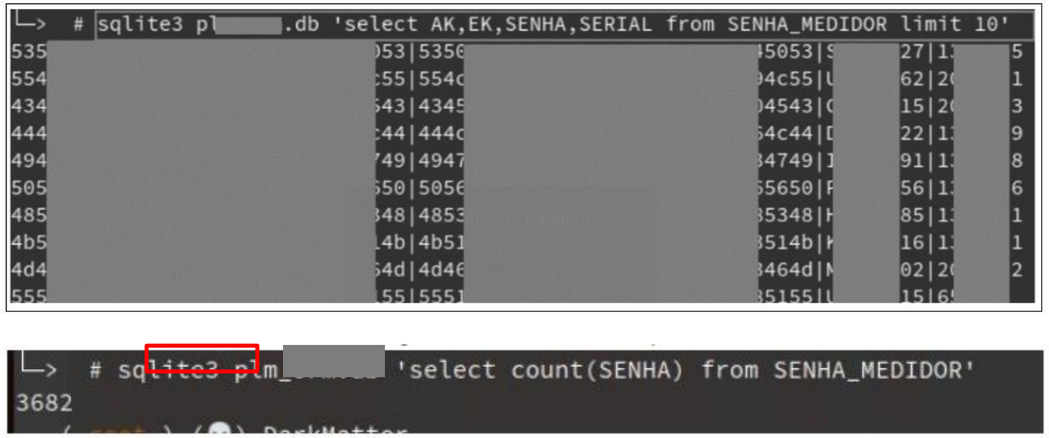
Resultados – Exemplo

Credenciais insuficientemente protegidas : Acesso não autorizado

- Analisamos o fluxo de dados através ["/senha-medidor?cod_unidade="] o qual é acionado sempre que uma conexão for estabelecida, constatou-se a possibilidade de interceptar os dados transmitidos.
- As informações incluem ID, senha de acesso, número serial do dispositivo e outros parâmetros relevantes de configuração
- Realizamos o download do arquivo de banco de dados com as senhas dos medidores da plataforma.



Detalhe do retorno em texto claro do endpoint



Amostra de registros

Este ataque nos concedeu acesso não autorizado ao dispositivo e eventualmente permitiria acesso não autorizado à um número elevado de dispositivos de medição. Tal acesso permite privilégio para execução de comandos de atuação, como o de corte de energia, além da troca da senha do dispositivo.

Discussão e Trabalhos Futuros

- A AMI enfrenta desafios significativos relacionados à segurança cibernética, decorrentes de sua natureza interconectada e arquitetura distribuída, que ampliam a superfície de ataque - uma característica da Internet das Coisas (IoT).
- As ocorrências das vulnerabilidades, majoritariamente pontuadas como de alta severidade, estão ligadas a falhas na gestão de acesso e identidade (IAM) e a fragilidades em interfaces para configuração e gerenciamento dos dispositivos de medição.
- Abordagens viáveis de mitigação para as vulnerabilidades identificadas foram apresentadas por trabalhos anteriores citados no artigo, incluindo:
    - Mecanismos de criptografia forte,
    - Uso de mecanismos de gerenciamento de chaves
    - Sistemas de Detecção de Intrusão
    - Revisões e auditorias regulares de segurança

- Este trabalho lança um alerta sobre a importância de desenvolver ações sistemáticas para reforçar a segurança cibernética de medidores inteligentes e indica um caminho para pesquisas futuras.