ANÁLISE DAS BASES DE VULNERABILIDADES CVE E CWE PARA IDENTIFICAÇÃO E CLASSIFICAÇÃO DE VULNERABILIDADES EM DISPOSITIVOS IOT

Amanda Helena Viscovini (PIC), Luciana Andréia Fondazzi Martimiano. E-mail: lafmartimiano@uem.br.

Universidade Estadual de Maringá, Centro de Ciências Exatas e da Terra, Maringá, PR.

Ciência da Computação/Sistemas de Computação

Palavras-chave: Segurança em Dispositivos IoT, Base de Vulnerabilidades, Base de *Exploits.*

RESUMO

A análise de vulnerabilidades permite examinar, sob determinadas circunstâncias, o comportamento de ambientes computacionais, identificando falhas que possam ser exploradas para a execução de um ataque. Para que seja possível identificar as vulnerabilidades, é preciso entender como elas são descritas e como podem ser utilizadas pelos atacantes. Neste sentido, as bases CVE *(Common Vulnerabilities and Exposures)* e CWE *(Common Weakness Enumeration)* são duas fontes ricas, enquanto a *Exploit-DB (Exploit Database)* complementa as informações ao fornecer exemplos de como vulnerabilidades podem ser exploradas. As bases são públicas e mantidas por diversas entidades, e, por meio delas, é possível encontrar informações para mitigar vulnerabilidades e melhorar a segurança dos ambientes computacionais. Em ambientes de Internet das Coisas (IoT), os dispositivos precisam ser analisados a fim de identificar quais vulnerabilidades podem estar presentes e, portanto, podem ser exploradas. Neste contexto, este relatório apresenta os resultados do estudo das bases CVE, CWE e Exploit-DB para encontrar e classificar vulnerabilidades em dispositivos IoT.

INTRODUÇÃO

Vulnerabilidades, em segurança da informação, são fraquezas ou falhas em um software, firmware ou hardware que são capazes de gerar danos à integridade, à

confidencialidade, à autenticidade e à disponibilidade. Segundo a norma ISO/IEC 27000 (2018), vulnerabilidade é definida como *"weakness of asset or control that can be exploited by one or more threats*", que em português significa: "fraqueza do ativo ou controle que pode ser explorada por uma ou mais ameaças". Já *exploits* são programas projetados por atacantes para explorar vulnerabilidades e podem resultar em roubos de dados, sequestros de informação, fraudes e prejuízos.

Neste contexto, a análise de vulnerabilidades desempenha um papel crucial na compreensão das fragilidades de sistemas computacionais, permitindo a detecção de falhas de segurança que podem ser exploradas por atacantes. Bases públicas como CVE *(Common Vulnerabilities and Exposures)* e CWE *(Common Weakness Enumeration*) representam recursos valiosos, fornecendo informações detalhadas sobre a descrição de vulnerabilidades. Além disso, a Exploit-DB *(Exploit Database)* complementa essas informações ao mostrar como as vulnerabilidades podem ser exploradas na prática.

Ambientes de Internet das Coisas (IoT) possuem dispositivos físicos interconectados que são usados cotidianamente e nesse contexto a segurança da informação é primordial. Portanto, é necessário analisar bases de vulnerabilidades para identificar e classificar quais vulnerabilidades podem ser encontradas, e exploradas, em dispositivo*s* IoT.

O objetivo principal deste projeto é analisar os resultados obtidos com o estudo das bases CVE *(Common Vulnerabilities and Exposures)*, CWE *(Common Weakness Enumeration) e* Exploit-DB *(Exploit Database)* para encontrar e classificar vulnerabilidades em dispositivos IoT.

MATERIAIS E MÉTODOS

Os principais materiais utilizados foram as bases CWE, CVE e Exploit-DB.

A CWE é uma base de dados pública que lista, de forma genérica, as categorias de vulnerabilidades de *hardware* e *software* conhecidas (https://cwe.mitre.org/). Já a CVE é uma base de dados que tem como objetivo descrever vulnerabilidades conhecidas publicamente de *softwares* disponíveis publicamente (https://cve.mitre.org/). Por fim, a Exploit-DB é uma base de dados de domínio público de *exploits* de vulnerabilidades encontradas em *softwares*, essa base é desenvolvida por pesquisadores de vulnerabilidades e testadores de invasão (https://www.exploit-db.com/).

O método utilizado foi o bibliográfico e está descrito a seguir. Em primeiro lugar, foram selecionadas, por meio de *strings* de buscas, apenas vulnerabilidades que ocorrem em dispositivos IoT das bases de dados. Na base CWE foi utilizada a *string "(vulnerability OR exploit OR attack OR weakness) AND (Internet of Things*

devices OR IOT *devices OR* IOT *OR Internet of Things)"*, durante o período de 14/12/2022 e 10/02/2023, que retornou 111 resultados. Contudo, alguns resultados eram *patchs* de atualização, coletâneas de registros, calendários de eventos ou notícias e esses foram descartados. Depois de selecionar os registros, eles foram estudados e traduzidos para o português.

O mesmo procedimento foi feito na base CVE, durante o período de 23/02/2023 e 26/02/2023, foi utilizada a *string* "*(Vulnerability OR exploit OR attack) AND (Internet of Things devices OR* IOT *devices)*", que retornou 13 resultados. Por conta do número de resultados ter sido pequeno, foram acrescentados os resultados da *string "(Vulnerability OR exploit OR attack) AND (*IOT *device)*", durante o período de 01/03/2023 e 23/03/2023, que retornou 131 registros. Depois de selecionar os registros da base CVE, eles foram estudados e traduzidos para o português.

Em seguida, cada registro das bases CWE e CVE foi classificado de acordo com seu tipo de vulnerabilidade, a fim de agrupar vulnerabilidades que fossem exploradas pelos mesmos *exploits*. Para cada categoria de vulnerabilidade, foram selecionados *exploits* da base *Exploit-DB* que fossem capazes de explorar as falhas.

RESULTADOS E DISCUSSÃO

O principal resultado do projeto foi uma tabela de correlações de categorias de vulnerabilidades, vulnerabilidades existentes e *exploits* que exploram as respectivas vulnerabilidades. A Tabela 1 mostra parte dessa tabela de correlações.

Tabela 1 - Correlação entre vulnerabilidades e *exploits* existentes para exploração

Tipo de Vulnerabilidade	Registro	*Exploits*
CSRF (falsificação de solicitações entre sites)	CWE-352, CVE-2020-3531, CVE-2018-0270	https://www.exploit-db.com/exploits/51388 https://www.exploit-db.com/exploits/50323
Integer Underflow	CWE-191	https://www.exploit-db.com/exploits/42946
Out-of-Bounds write	CVE-2021-21280, CVE-2020-11267	https://www.exploit-db.com/exploits/47119
Acesso de caminho absoluto	CWE-36	https://www.exploit-db.com/exploits/31708

CONCLUSÕES

Este resumo apresenta os resultados da análise das bases CWE e CVE, correlacionando tipos de vulnerabilidades com *exploits* da base Exploit-DB. Considera-se que o objetivo proposto para o projeto foi cumprido e por meio dele foi

possível estudar diversas vulnerabilidades e como elas podem ser exploradas. Com trabalho futuro, sugere-se a implementação de propostas de intervenção capazes de minimizar os danos gerados pelas falhas de segurança em dispositivos IoT e testes de invasão usando os *exploits* selecionados.

REFERÊNCIAS

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000:2018 - *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. *5th ed. Geneva:* ISO, 2018.

CWE. ***Common Weakness Enumeration*.** Disponível em: https://cwe.mitre.org/. Acesso em: 16 de janeiro de 2023.

CVE. ***Common Vulnerabilities and Exposures*.** Disponível em: https://cve.mitre.org/. Acesso em: 23 de fevereiro de 2023.

EXPLOIT-DB. ***Exploit Database.*** Disponível em: https://www.exploit-db.com/. Acesso em: 30 de maio de 2023.