Community Based Platform for Vulnerability Categorization

Jana Komárková, Lukáš Sadlek, Martin Laštovička

Institute of Computer Science, Faculty of Informatics
Masaryk University, Brno, Czech Republic

{komarkova, lastovicka}@ics.muni.cz, sadlek@mail.muni.cz

Abstract

Many approaches, such as attack graphs, require knowledge of vulnerability's properties such as impact, prerequisities, and exploitability. Currently, those properties are either categorized manually or too roughly. We present a program for granular, automated categorization of vulnerability. Further, we present a platform supporting researchers by gathering and sharing both raw and categorized data about vulnerabilities and community labeled datasets. The source code of our categorization program is available on GitHub at https://github.com/CSIRT-MU/VulnerabilityCategorization.

Features

Vulnerability Information
The accumulated raw information about vulnerabilities gathered from various publicly available sources is provided in JSON. We are developing tools to include more sources, such as vendor official vulnerability reports. The information is sorted by CVE id.

Categorized Vulnerabilities
For each vulnerability, its likelihood of exploit, prerequisities and impact of exploit are categorized and the results are available in JSON. The vulnerability characteristics are categorized using a proof-of-concept algorithm described in the chart below. The algorithm will be improved on in future based on gathered data.

Feedback
The platform enables the community to give feedback with respect to the correctness of the categorized information, thus providing the measure of efficiency of current approach and labeled data for further development of vulnerability characteristics categorization tools. It will be used to extend the categorized data by indication of the correctness.

Labeled Data
The feedback is also used for creation of dataset with labeled vulnerabilities, which will be provided for general usage. This will help development of more accurate categorization methods.

Vulnerability Characteristics

We identified three main properties that could researchers find useful: impact, prerequisities, and likelihood of successful exploit. We formed categories for each characteristics as follows:

Impact
- arbitrary code execution as root/administrator/system
- gain root/system/administrator privileges on system
- privilege escalation on system
- gain user privileges on system
- arbitrary code execution as user of application
- gain privileges on application
- system integrity/availability/confidentiality loss
- application integrity/availability/confidentiality loss
- communication integrity/availability/confidentiality loss

Prerequisities
- local access
- local access, user privileges
- local access, root/administration/system privileges
- remote access
- remote access, user privileges
- network access, root/administration/system privileges
- physical access

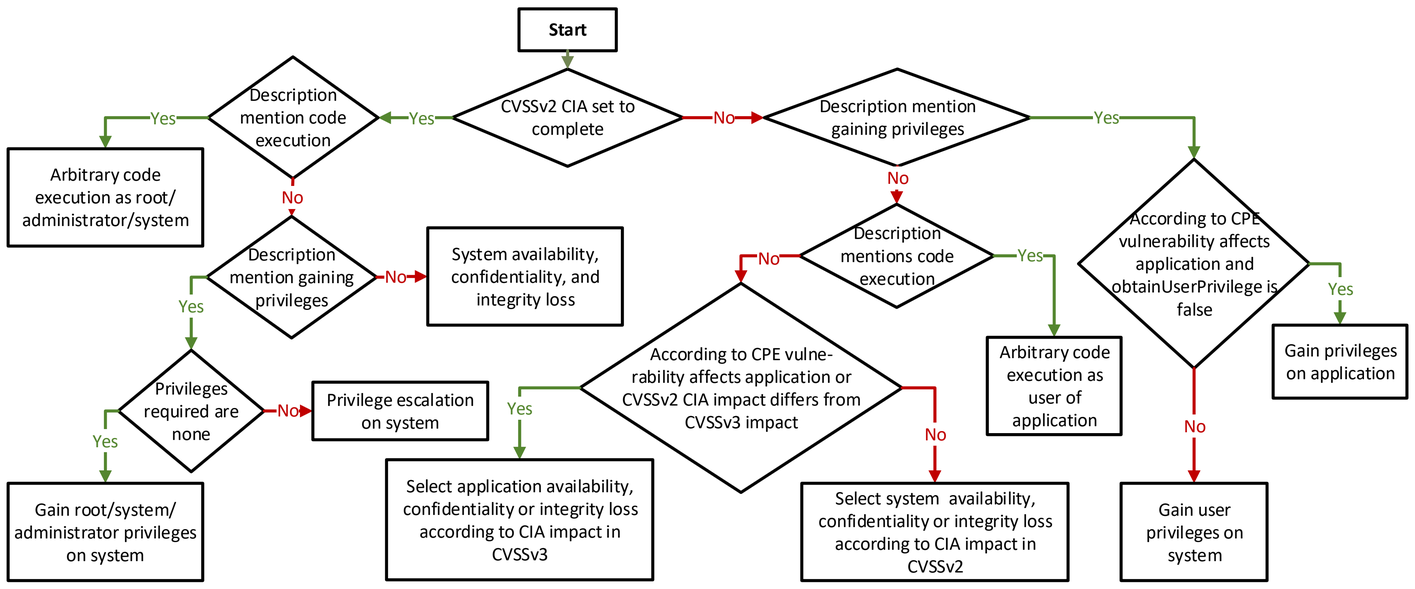
Likelihood
- low
- medium
- high

Vulnerability Categorization Chart

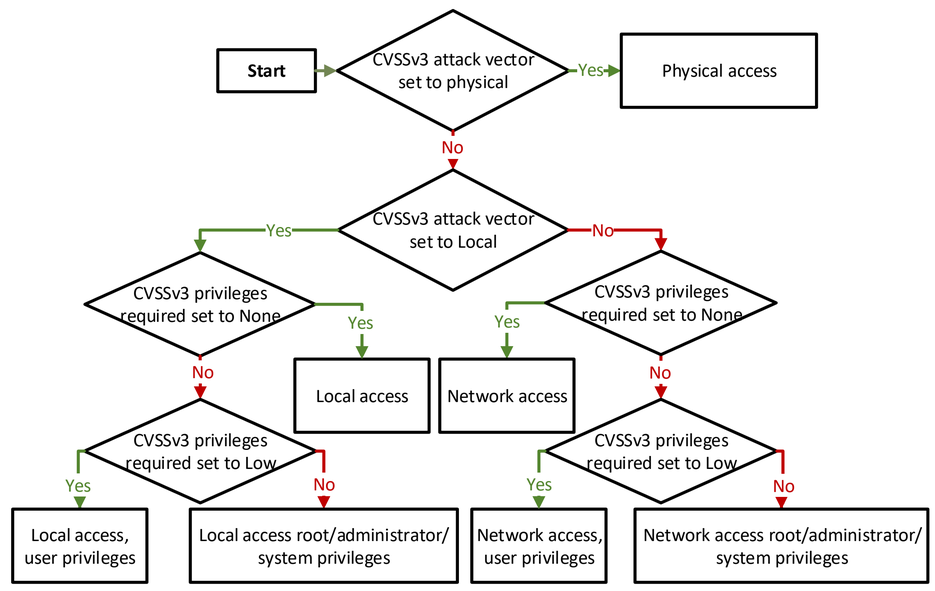
The decision chart of a proof-of-concept program for vulnerability characteristics categorization. The program uses CVSSv2, CVSSv3, CPE and text description to derive the impact, prerequisities and likelihood of vulnerability's exploit.

The impact categorization utilizes a differences between CVSSv2 and CVSSv3 methodologies, namely that the CVSSv3 impact is related to the actual source of the vulnerability (i.e. OS, software) and CVSSv2 impact is related to the whole system. The prerequisities are categorized based on attack/access vector (CVSSv3/CVSSv2) and privileges required (CVSSv3). The probability of successful exploit is estimated based on attack/access complexity (CVSSv3/CVSSv2) and user interaction (CVSSv3).

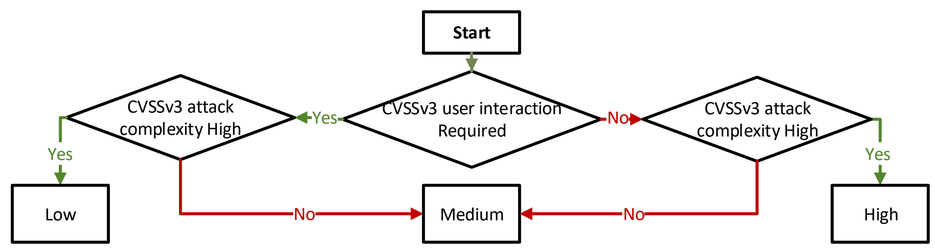
Impact Categorization



Prerequisities Categorization



Likelihood Categorization



Acknowledgement

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20172020070 Research of Tools for Cyber Situational Awareness and Decision Support of CSIRT Teams in Protection of Critical Infrastructure.

Martin Laštovička is Brno Ph.D. Talent Scholarship Holder – Funded by the Brno City Municipality.

CSIRT-MU