

Datasets for vulnerabilities detection in IoTs operating systems and applications

Anonymous for review

ABSTRACT

TBA

KEYWORDS

Cybersecurity, Internet of Things, IoT security, Smart Environments, Machine Learning, Natural Language Processing;

ACM Reference Format:

Anonymous for review . 2023. Datasets for vulnerabilities detection in IoTs operating systems and applications. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, ?? pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUCTION

The Internet of Things (IoT) refers to the growing interconnected physical devices, components, vehicles and home appliances to the internet [oracle2023:what]. These connected devices exchange information to ease our day-to-day lives, business and industries. However, these devices continue to pose security issues and vulnerabilities over the years.

2 RELATED WORK

Al-Boghdady et al. [al-boghdady2022:idetector] have created a tool called iDetect for detecting vulnerabilities in the C/C++ source code of IoT operating systems (OSs). The labeling of the dataset was done using static code analyzing tools (SATs); Cppcheck version 2.1 [cppcheck2.12021:tool], Flawfinder version 2.0.11 [dwheeler2011:flawfinder] and Rough Auditing Tool for Security (RATS) [rats2021:rough].

3 THE PROPOSED FRAMEWORK:

4 DATASET ANALYSIS:

5 CONCLUSION AND FUTURE WORK

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Conference'17, July 2017, Washington, DC, USA

© 2023 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>

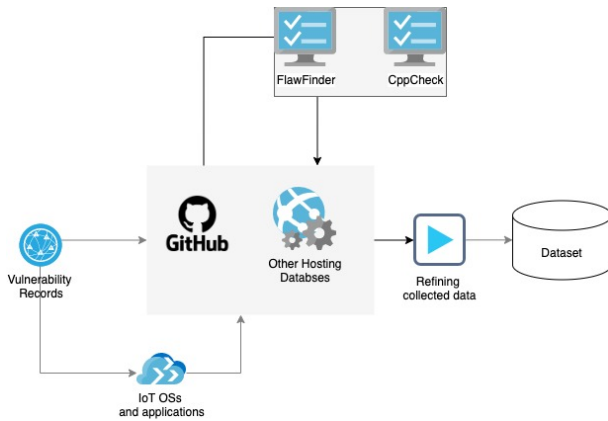


Figure 1: The proposed framework for vulnerability data collection

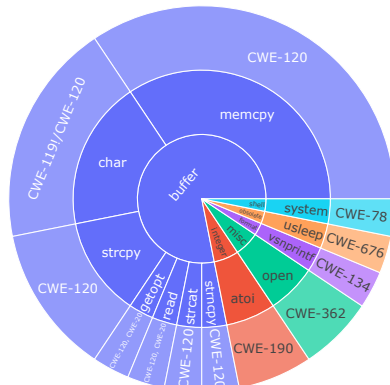


Figure 2: The sunburst chart showing the frequency of vulnerability categories, names and CWEs

urls	count
http://www.securityfocus.com/	222
http://www.oracle.com/	177
http://www.securitytracker.com/	127
http://www.mandriva.com/	25
http://www.zerodayinitiative.com/	24
http://www.ubuntu.com/	14
http://www.vupen.com/	11
http://www.openwall.com/	6
http://www.exploit-db.com/	5
http://www.ibm.com/	4
http://www.ti.com/	3
http://www.lutron.com/	3
http://www.vmware.com/	3
http://www.gedigitalenergy.com/	2
http://www-01.ibm.com/	2
http://www.accuenergy.com/	2
http://www.telink-semi.com/	2
http://www.solarwinds.com/	1
http://www.fortiguard.com/	1
http://www.redhat.com/	1

Table 1: Summary of the top databases hosting vulnerability records of IoT OSs and applications