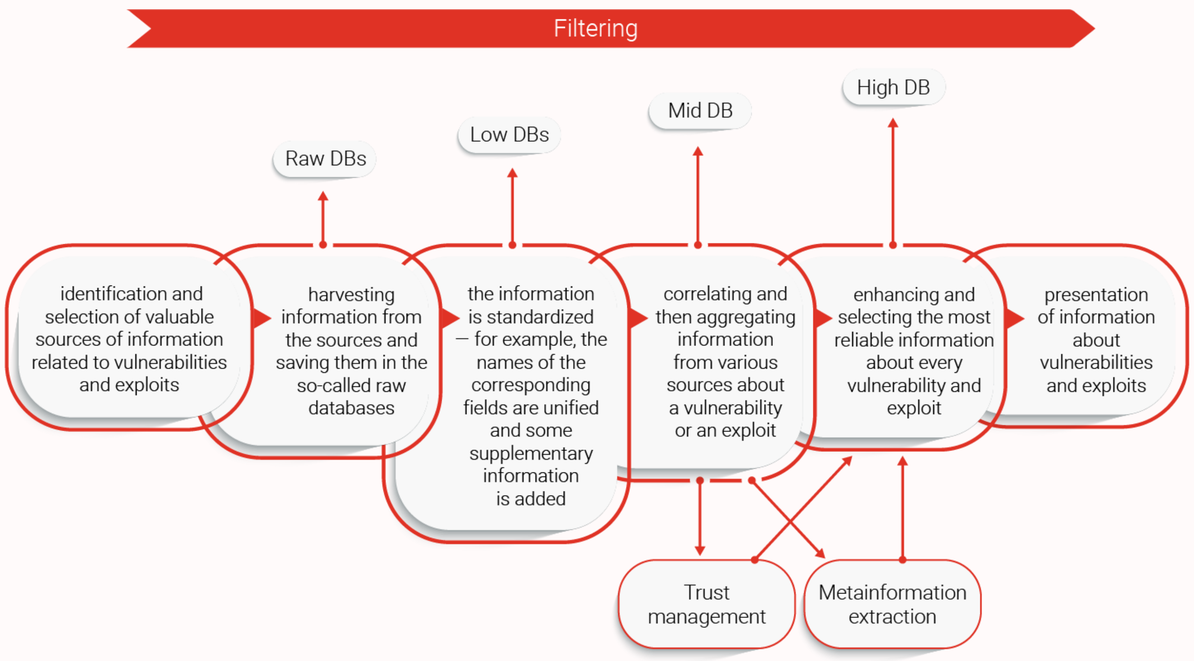
A Repository of Actionable Information on the Internet of Things

Anna Felkner and Marcin Rytel
NASK - Research and Academic Computer Network
email: anna.felkner@nask.pl

Abstract

The poster presents the process of creating a database containing publicly available information about vulnerabilities and exploits affecting the Internet of Things devices. Over 100 unique sources of different types were analysed (structured databases, vendor bulletins, reports, blogs or individual websites). The extracted information was standardised, aggregated, correlated and enriched to provide a rich source of actionable information related to IoT. This information is extremely useful not only to device users, but also to CSIRTs (Computer Security Incident Response Teams) and network owners.

Database creation

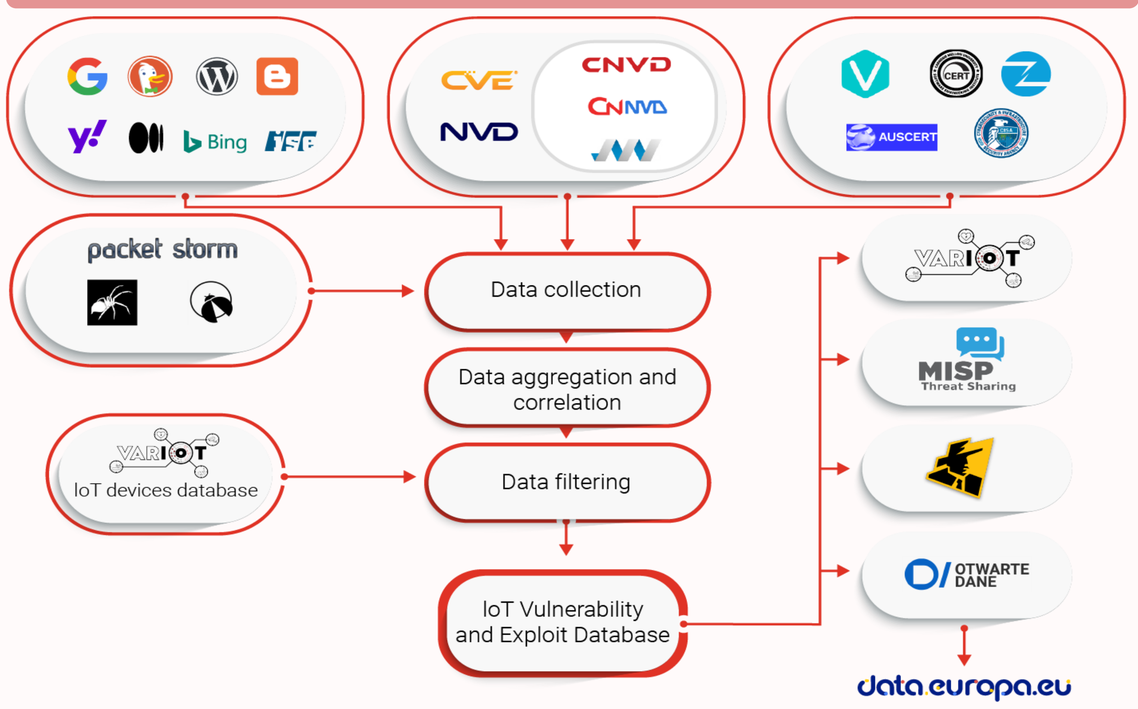


Information sources

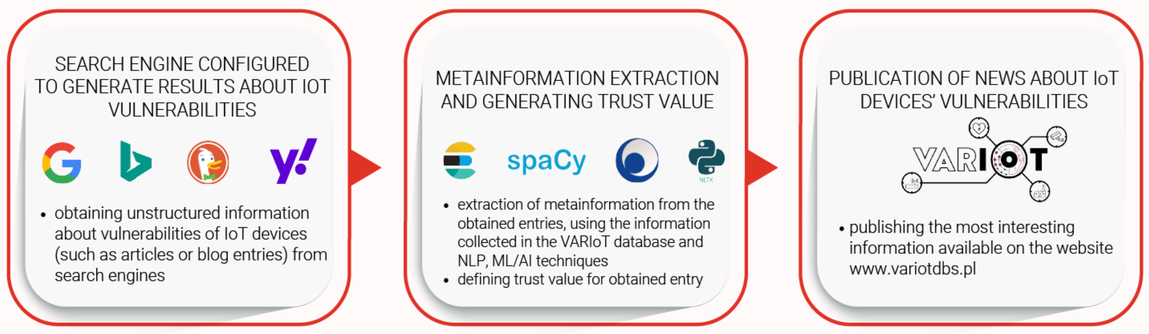
Short Name	Full Name	Type of database
BID	SecutiryFocus Bugtraq	Vulnerability/Exploit
CERT/CC	Carnegie Mellon University CERT Coordination Center	Vulnerability
CNNVD	Chinese National Database of Information Security	Vulnerability
CNVD	China National Vulnerability Database	Vulnerability
Exploit-DB	Exploit Database by Offensive Security	Exploit
IVD	ICS Vulnerability Database	Vulnerability
JVNDB	Japan Vulnerabilities Notes Database	Vulnerability
NVD	National Vulnerability Database	Vulnerability
Packet Storm	Packet Storm Security	Vulnerability/Exploit
Vulmon	Vulmon Vulnerability Search Engine Vulnerability	Vulnerability
VUL-HUB	VUL-HUB Information Security Vulnerability Portal	Vulnerability
ZDI	Zero Day Initiative	Vulnerability
ZSL	Zero Science Lab	Vulnerability

Number of unique IDs in low databases

Database architecture

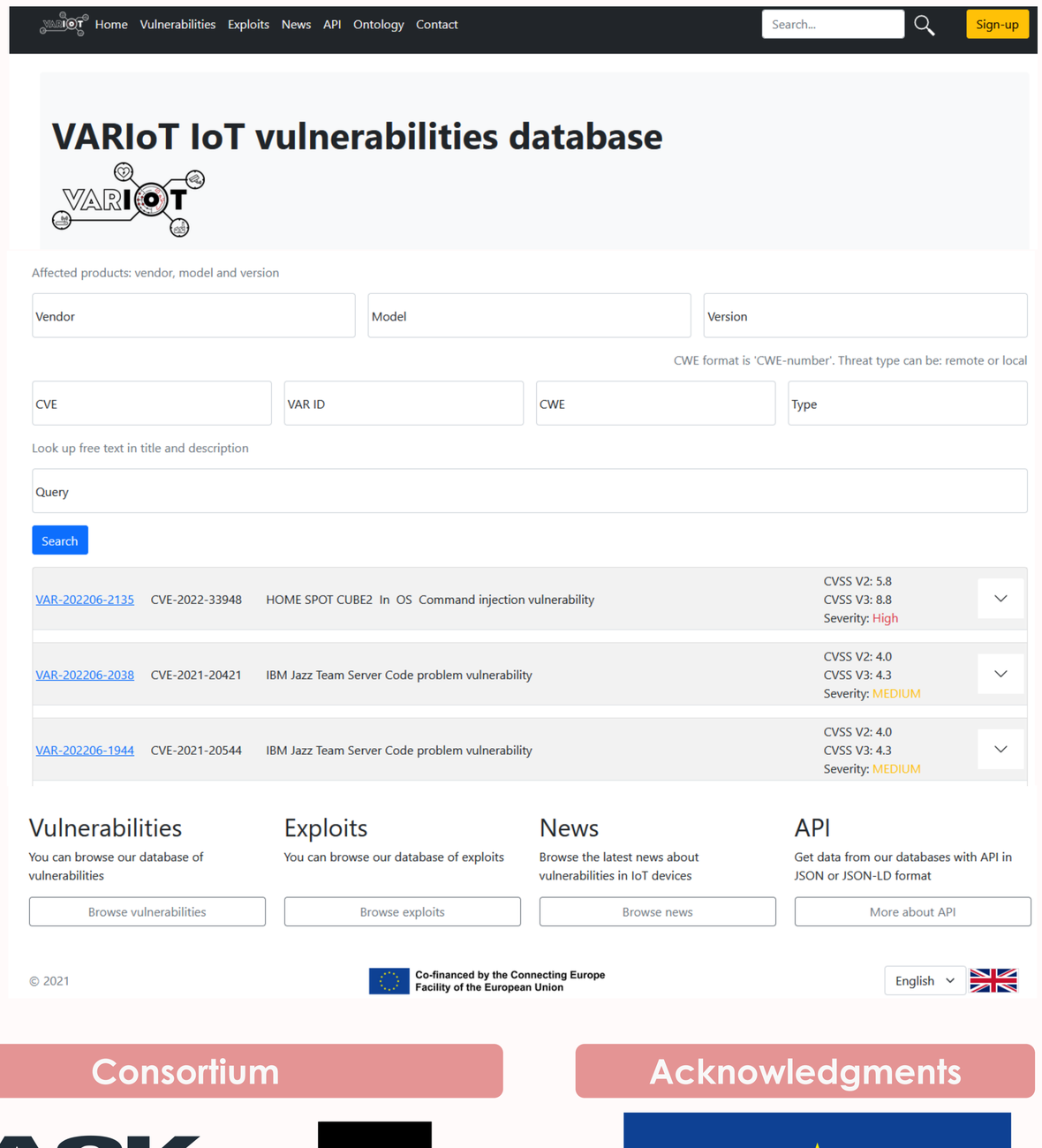


Search engine



Data publication

The repository is accessible through its dedicated portal: https://www.variotdbs.pl/, as well as through the European Data Portal: data.europa.eu and through the Polish Open Data Portal: https://dane.gov.pl/en.



Our websites

https://variot.eu

https://variotdbs.pl

Consortium

NASK
TELECOM SudParis
SHADOWSERVER
IP PARIS
Mondragon Unibertsitatea
CIRCL Computer Incident Response Center Luxembourg

Acknowledgments

Co-financed by the Connecting Europe Facility of the European Union and by the program of the Minister of Science and Higher Education entitled "PMW" in the years 2020–2022