FOSDEM 2022

Finding vulnerabilities using CVE-BIN-TOOL

Summary

- Introduction to CVE Bin Tool
- Architecture
- Scanning approach
- Use Cases
- Future Roadmap

CVE-Bin-Tool

- Why?
- First released in 2019 from Intel
- Released under GPL 3.0
- Primarily targeted at Linux platforms
- Part of Python Software Foundation GSOC projects in 2020 and 2021
- Multiple reporting formats including CSV, HTML and PDF
- Latest release 3.0 (December 2021) available from PyPi

Two modes of use

- A binary scanner which helps you determine which packages/libraries may have been included as part of a software component
- Tool for scanning known component lists in various formats
  - Simple .csv list
  - Several Linux distribution package lists
  - Several Software Bill of Materials (SBOM) formats

- Both produce a list of components with reported CVEs and associated severity

- Report Generated: 2022-01-08 14:13:28
- Time of last update of CVE Data: 2022-01-07 22:52:22

CVE SUMMARY

Severity	Count
CRITICAL	12
HIGH	43
MEDIUM	17
LOW	4

NewFound CVEs

Vendor	Product	Version	CVE Number	Severity	Score (CVSS Version)
alpinelinux	apk-tools	2.10.4	CVE-2021-30139	HIGH	7.5 (v3)
busybox	busybox	1.30.1	CVE-2018-1000500	HIGH	8.1 (v3)
busybox	busybox	1.30.1	CVE-2021-42374	MEDIUM	5.3 (v3)
busybox	busybox	1.30.1	CVE-2021-42376	MEDIUM	5.5 (v3)
busybox	busybox	1.30.1	CVE-2021-42378	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42379	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42380	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42381	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42382	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42384	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42385	HIGH	7.2 (v3)
busybox	busybox	1.30.1	CVE-2021-42386	HIGH	7.2 (v3)

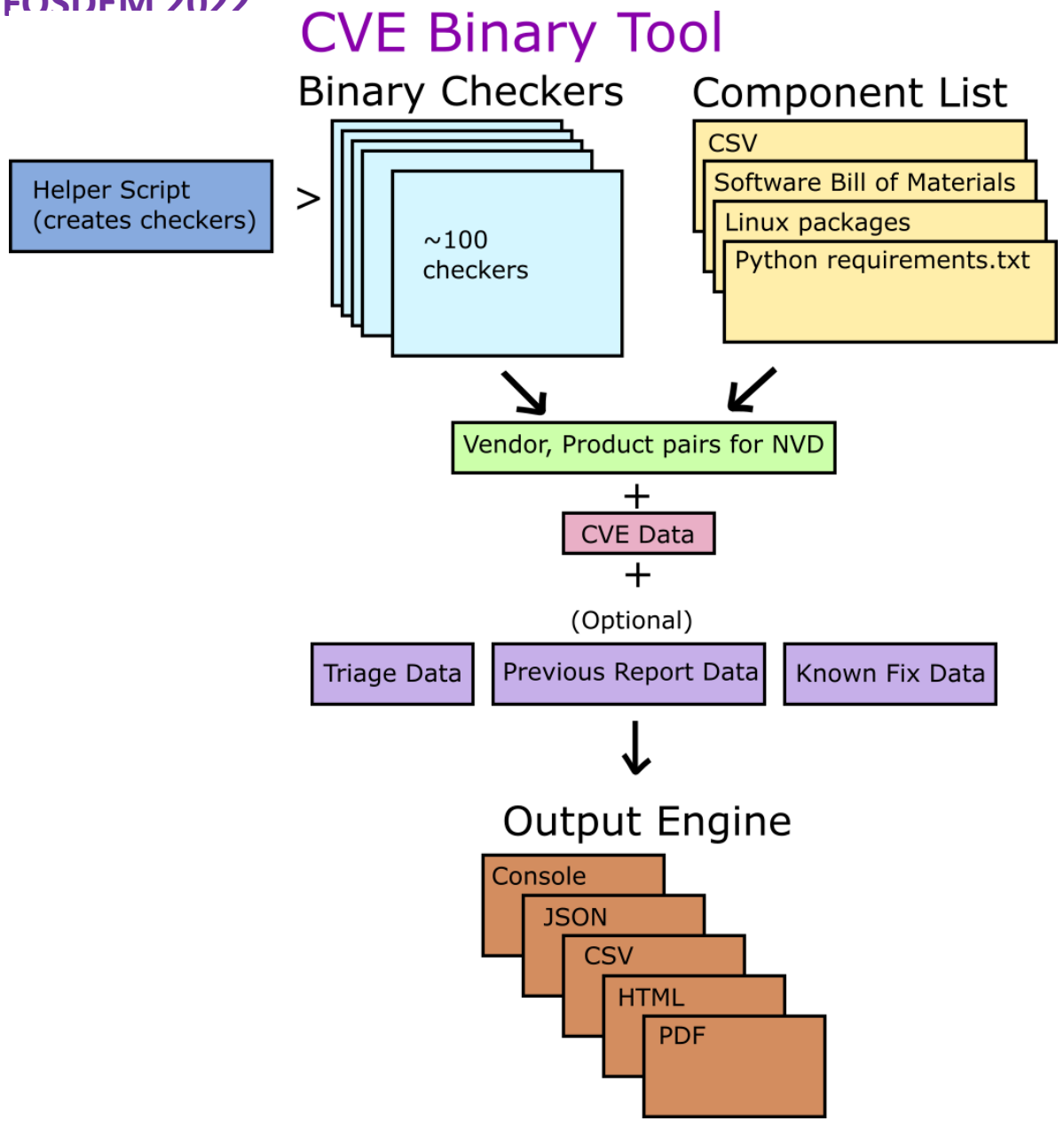
Development Process

- Python 3 (3.7+)
- Tested under Windows and Ubuntu
- Code quality – isort, black, flake8, bandit, pyupgrade
  - LGTM quality A+
- Adopted 'Conventional Commits' in 2021
- Adoption of OpenSSF best practices in progress

- https://cve-bin-tool.readthedocs.io/en/latest/CONTRIBUTING.html

Architecture

- Uses local copy of NVD database
  - can operate offline



Scanning for Vulnerabilities in Libraries

- Uses the utility *strings* on a binary file
- Various patterns are used to match product name and extract version information
- Matched patterns are then used to interrogate the local copy of the NVD database
  - Product and Vendor pairs

Generic Binary Checkers format

- Every checker contains:
  - CONTAINS_PATTERNS - list of commonly found strings in the binary of the product
  - FILENAME_PATTERNS - list of different filename for the product
  - VERSION_PATTERNS - list of version patterns found in binary of the product.
  - VENDOR_PRODUCT - list of vendor product pairs for the product as they appear in NVD.
- Patterns supports regex to cover wide range of use cases
- Helper script developed during GSOC in 2021
- https://github.com/intel/cve-bin-tool/tree/main/cve_bin_tool/checkers

Available Checkers

accountsservice, avahi, bash, bind, binutils, bolt, bubblewrap, busybox, bzip2, cronie, cryptsetup, cups, curl,dbus, dnsmasq, dovecot, dpkg, enscript, expat, ffmpeg, freeradius, ftp, gcc, gimp, glibc, gnomeshell, gnupg, gnutls, gpgme, gstreamer, gupnp, haproxy, hdf5, hostapd, hunspell, icecast, icu, irssi, kbd, kerberos, kexectools, libarchive, libbpg, libdb, libgcrypt, libical, libjpeg_turbo, liblas, libnss, libsndfile, libsoup, libssh2, libtiff, libvirt, libvncserver, libxslt, lighttpd, logrotate, lua, mariadb, mdadm, memcached, mtr, mysql, nano, ncurses, nessus, netpbm, nginx, node, ntp, open_vm_tools, openafs, openjpeg, openldap, openssh, openssl, openswan, openvpn, p7zip, pcsc_lite, pigz, png, polarssl_fedora, poppler, postgresql, pspp, python, qt, radare2, rsyslog, samba, sane_backends, sqlite, strongswan, subversion, sudo, syslogng, systemd, tcpdump, trousers, varnish, webkitgtk, wireshark, wpa_supplicant, xerces, xml2, zlib, zsh

Use Case: Scan Downloaded Components

- Understand vulnerabilities within the Supply Chain

- Scan Python application dependences
  - More language scanners coming (Java, Javascript, Go)

Use Case: Scan Product Delivery

- Understand vulnerability status of a product delivery

- Scan delivery directory (recursively)
  - Deep scanning of archives (rpm, tar, etc)

Use Case: Scan Containers

- Integrated with TERN https://github.com/tern-tools/tern

- See also SBOM scanning

Use Case: Scan Linux Environment

- Scan local environment for vulnerabilities
- Supports Debian (.deb) and Red Hat (.rpm) distributions
- Identify potential packages to be updated where fixes are available

Use Case: Scan SBOM

- Consume SBOM file and report vulnerabilities
  - SPDX (multiple formats supported)
  - CycloneDX (JSON and XML)
  - SWID
- Works with SPDX version 2.2 and CycloneDX version 1.3

- Can consume SBOM files generated by TERN

Caution

- Running the tool does not guarantee that it will detect all of the vulnerabilities
  - Dependent on the checkers which are available/selected and if there isn't a checker for a specific library, vulnerabilities in that library will not be detected
- It does not guarantee that any of the reported vulnerabilities are present/exploitable.
  - As with all tools there will be some false reporting, both positive and negative although this can be controlled via the triage report which allows some reported CVEs to be suppressed.
- Important to keep the vulnerability database up to date.

RoadMap

- A list of good ideas is maintained
  - https://github.com/intel/cve-bin-tool/issues/1379
  - https://github.com/intel/cve-bin-tool/issues/1462 - to start GSOC project

- Ideas include:
  - More language/package manager scanners
  - Link to more vulnerability databases e.g. https://osv.dev/
  - UI

Take Aways

- One stop shop for vulnerability scanning with multiple use cases
  - for binaries, linux distributions and SBOMs

- Contributing to CVE-Bin-Tool
  - More Checkers
  - More Language/Package manager scanners
  - More Tests
  - More Documentation
  - https://goodfirstissue.dev/

Resources

- https://github.com/intel/cve-bin-tool
- https://readthedocs.org/projects/cve-bin-tool/

Thank You