RSA Conference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SPS-W05

Effective Software Supply Chain Monitoring

Michael F. Angelo – CRISC, CISSP

Chief Security Architect
Micro Focus | NetIQ
@mfa0007

Agenda

- The Problem
- Data Collection Strategy
- Analysis
- Suggestions for implementation…

The Problem – Corporate Consumption…

Water

Nutrition Facts

Serving Size 8oz Container Size (8oz)
Servings Per Container 2

Amount Per Serving	
Calories 0	Calories from Fat 0
	% Daily Value
Total Fat 0g	**0%**
Saturated Fat 0g	**0%**
Cholesterol 0mg	**0%**
Sodium 0mg	**0%**
Total Carbohydrates 0g	**0%**
Dietary Fiber 0g	**0%**
Sugars 0g	**0%**
Protein 0g	**0%**

Improved Water

Corporate Consumption

Doesn’t Matter

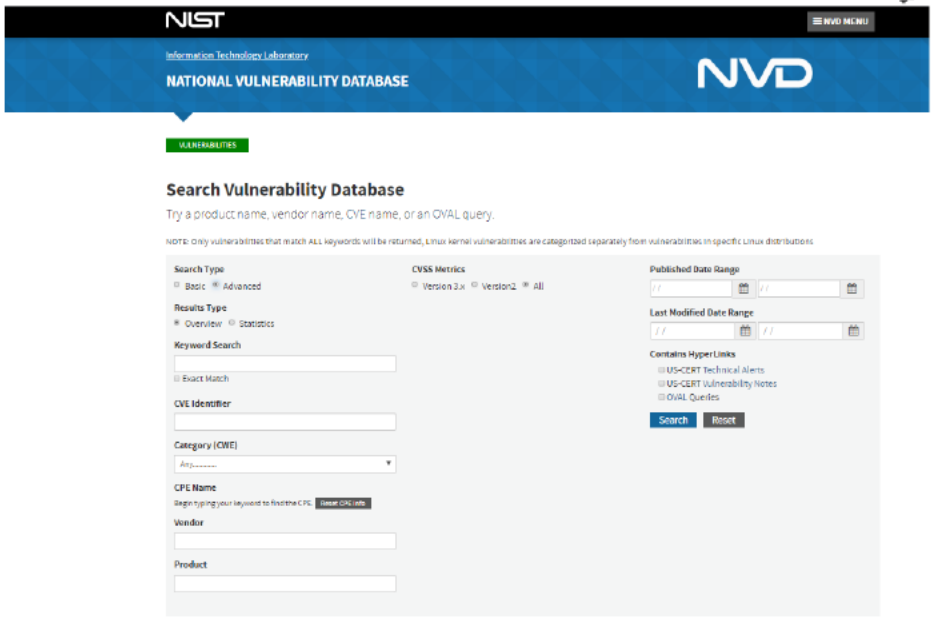
Problem #1?

- How do we know what applications are in our environment?
- What vulnerabilities do they have?
  - We can track what is installed in our environment.
  - We can monitor those applications via the NVD.
- Purchase tools to solve the problem…
  - Need source code.
  - Pay $$$$$ for binary analysis?
- Do it yourself…

Manual Product Analysis

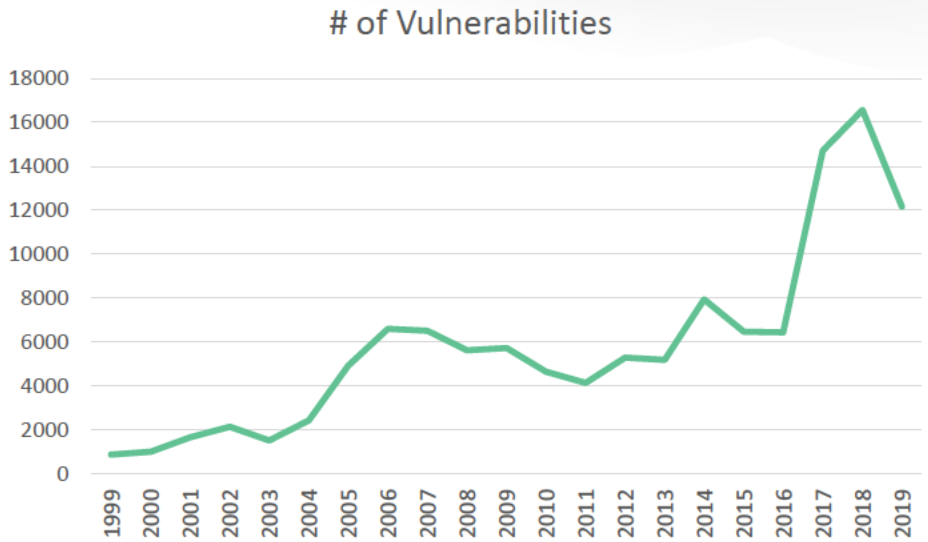
- Identify products
  - Copyright / Trademark / Version information
  - license files
  - Hashes
- Assuming all components are identified
  - Name, Origin, Version
  - Can associate to product

Next Find Vulns - NVD



https://nvd.nist.gov/vuln/search

Seems to be Working?



https://www.cvedetails.com/browse-by-date.php

Component Issue

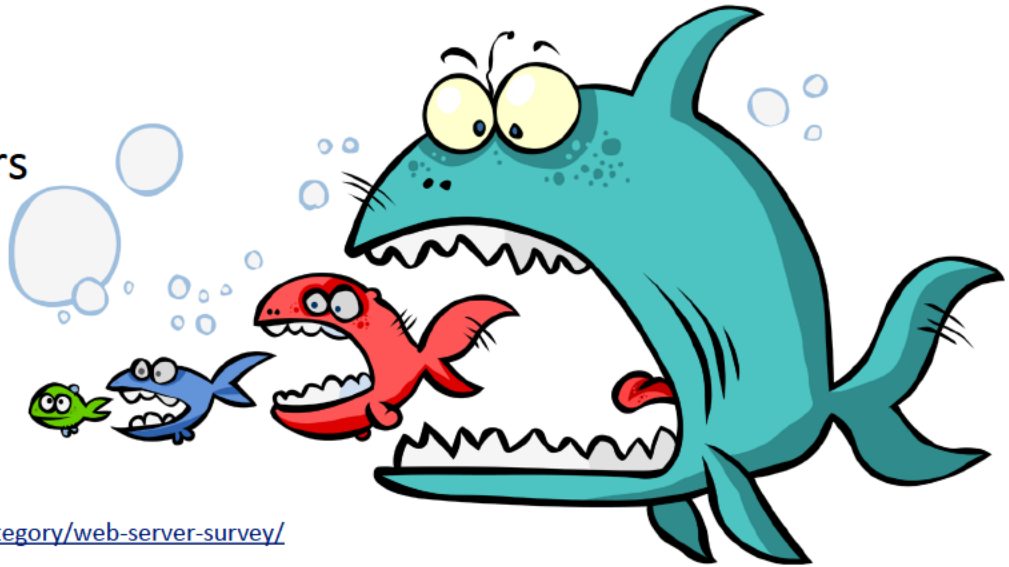
324 OpenSSL Vulns

3208 Products,
with SSL
as component

[1] https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=SSL&search_type=all

The Real Component Issue

- 2014 CNN $\frac{2}{3}$ web servers / sites used OpenSSL
- 2020 March[1]
  - 1,263,025,546 sites
  - 9,659.223 web facing computers



[1] https://news.netcraft.com/archives/category/web-server-survey/

Components in Products

- Look at install list, doesn't drill down
- FREE - OWASP Dependency Checker
- Build your own:
  - NIST Software Reference Library
  - Tools that are already build on it: NSRLSVR, NSRLLOOKUP

- OWASP Dependency Checker: https://owasp.org/www-project-dependency-check/
- NIST Library: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download
- Nsrlsvr (https://rjhansen.github.io/nsrlsvr/)
- Nsrllookup (http://rjhansen.github.io/nsrllookup/)

Product Component Declarations

- Internal Software
  - Require teams to declare it
  - Provide Automation Tools as applicable.
- External Software
  - Ask for a BoM

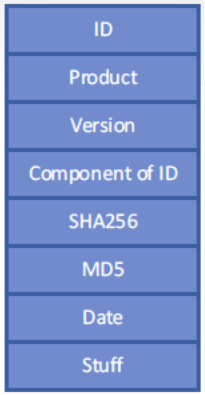
Supply Chain Not Solved

What About

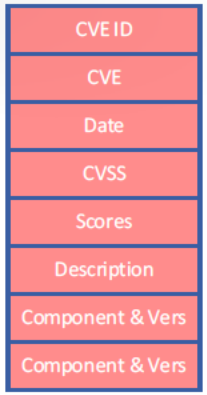
- Tracking vulnerabilities in components after tools are deployed?
- Need a New Tool
  - cross reference software to vulnerability in databases
  - raise awareness
  - provide sufficient information to enable you to test or ask about the Potential Security Vulnerability (PSV)
- The rest of the presentation will cover the lessons learned and gotcha's in developing a local tool.

Elements of a Solution

- Local database
- Applications
  - Components
- CVEs with component list
- Stuff
  - license references for applications and components

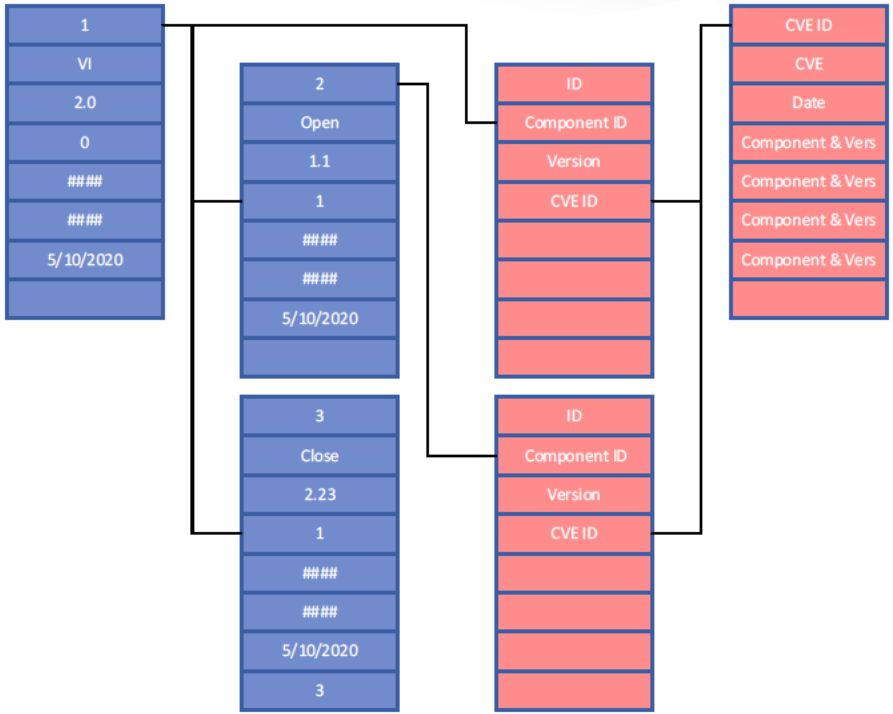


Product Table



CVE Table

Relationships

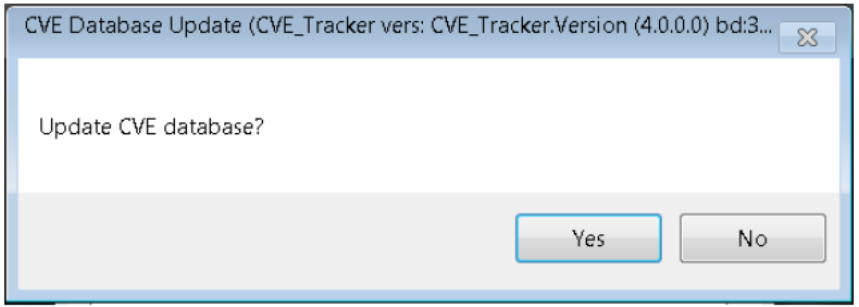


Procedurally

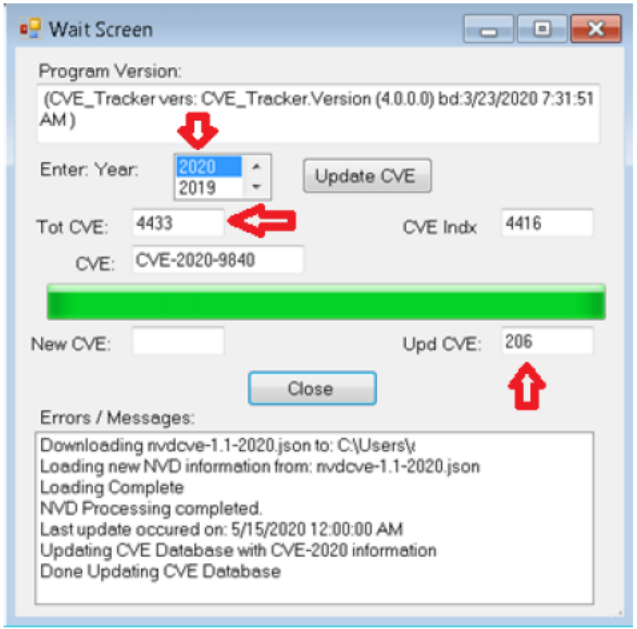
- Need to Load new CVEs daily
  - Need to review old products for new CVEs every day.
- Need to detect new products on systems.
  - Need to review new product against known CVEs.
- Need to notify ‘someone’ of:
  - New products & Components
  - CVEs associated with new products / components
- Provide triage mechanism

Update the CVE List

Always Ask

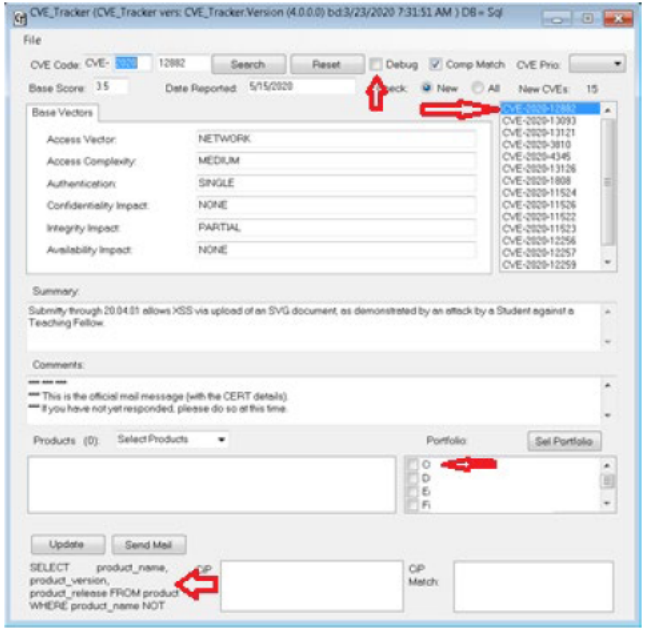


Download Screen

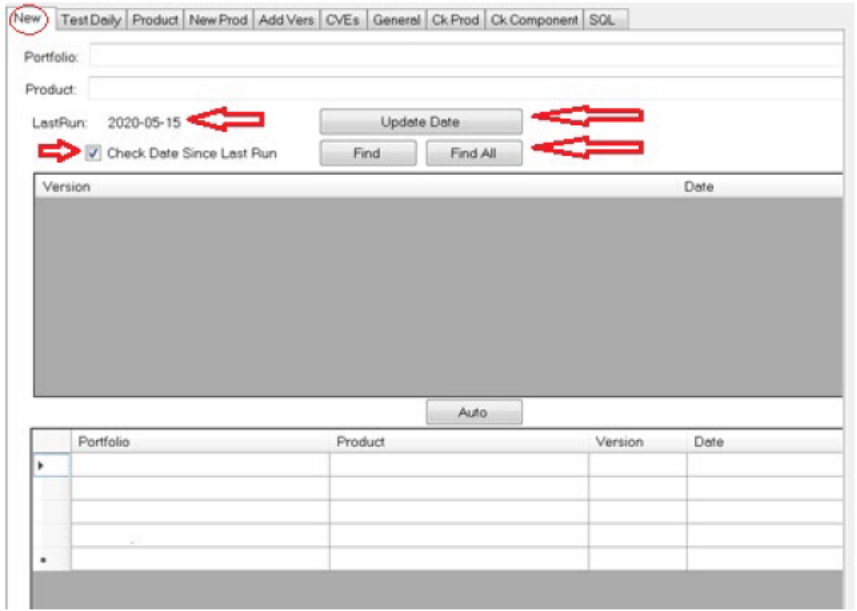


Thoughts

Top Screen

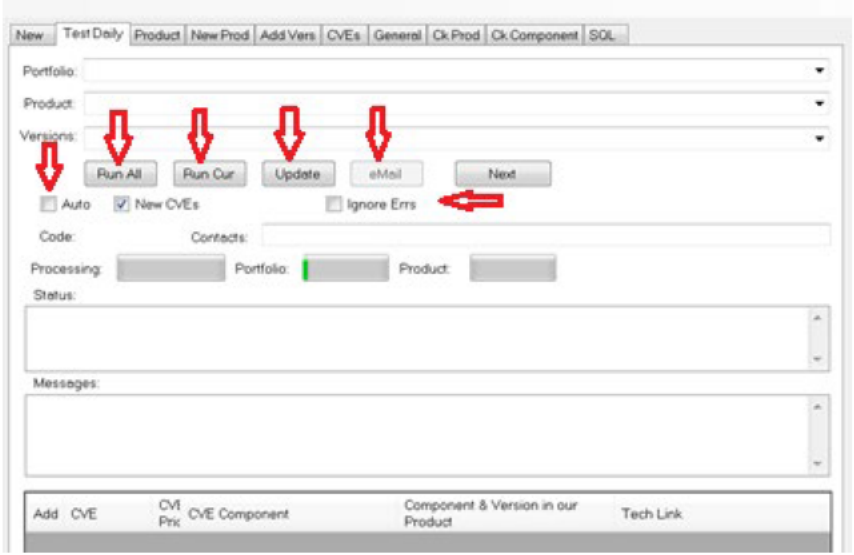


New Product List

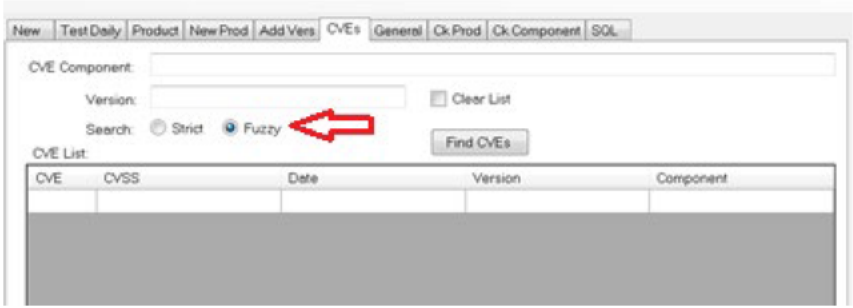


Next Step: Build a Proof of Concept

Daily Test

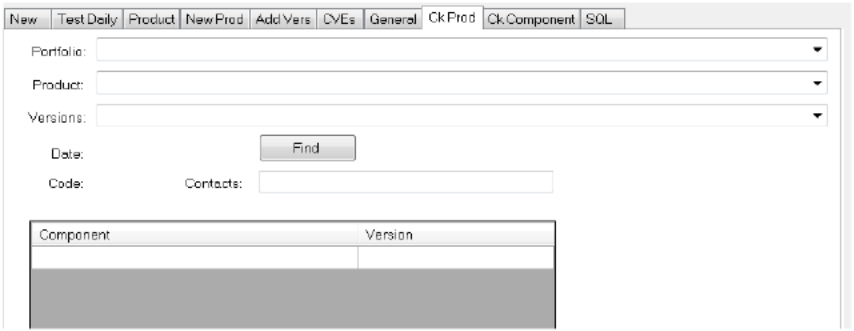


CVE List by Component

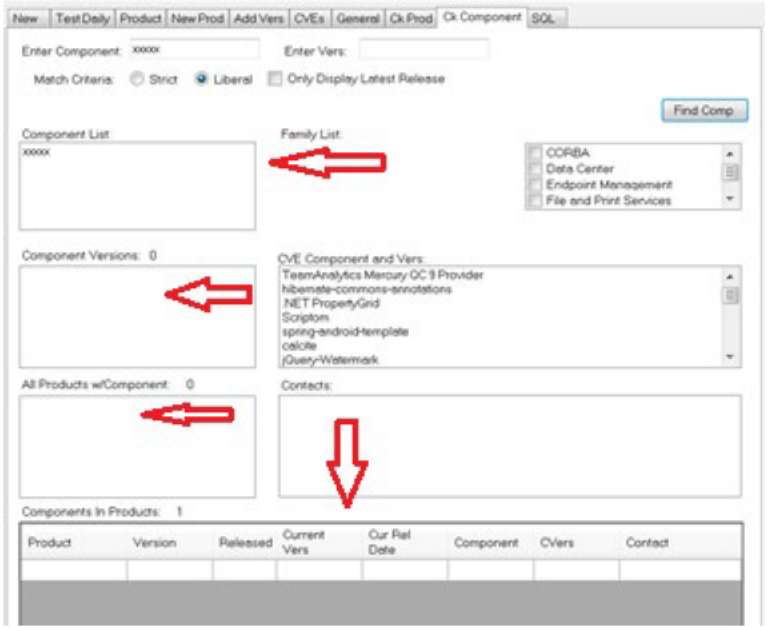


Eventually…

list of components in products



Components CVEs, Products, Mach

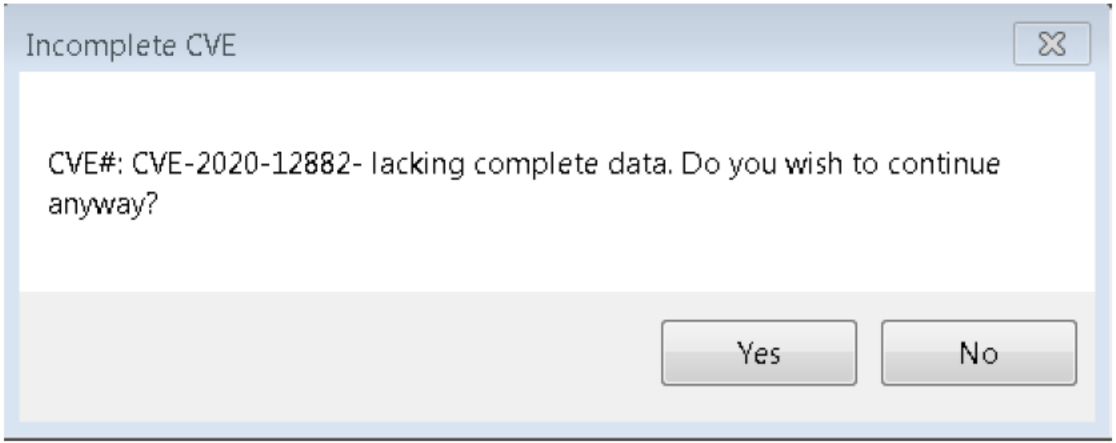


Caution

- Not every Vulnerability will be meaningful
- Every CVE would be marked as
  - Relevant, Not Relevant, Investigation
  - Mitigated, Not Mitigated, No mitigation needed

Issues….

- Version #s
- NVD data format changes
- Incomplete Informa



Re-Cap Applying This Today

- Look at resources in this presentation
- Create a tool that:
  - Identifies components in software
  - Checks against CVE
  - Enables triage & communication of potential issues
- Spread the word &

Remember

Don’t Poison Your Organization

RSAConference2020 APJ

A Virtual Learning Experience

Thank You

Michael F. Angelo – CRISC, CISSP
Chief Security Architect
Micro Focus | NetIQ
Michael.Angelo@Microfocus.com or Michael.Angelo@netiq.com
@mfa0007