

RSA® Conference 2020 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

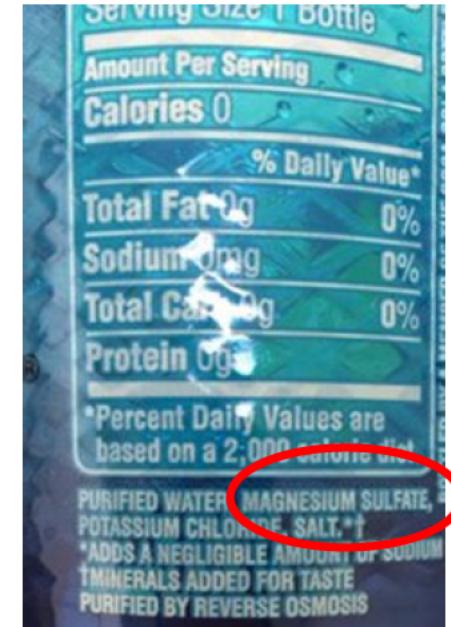
Nutrition Facts

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

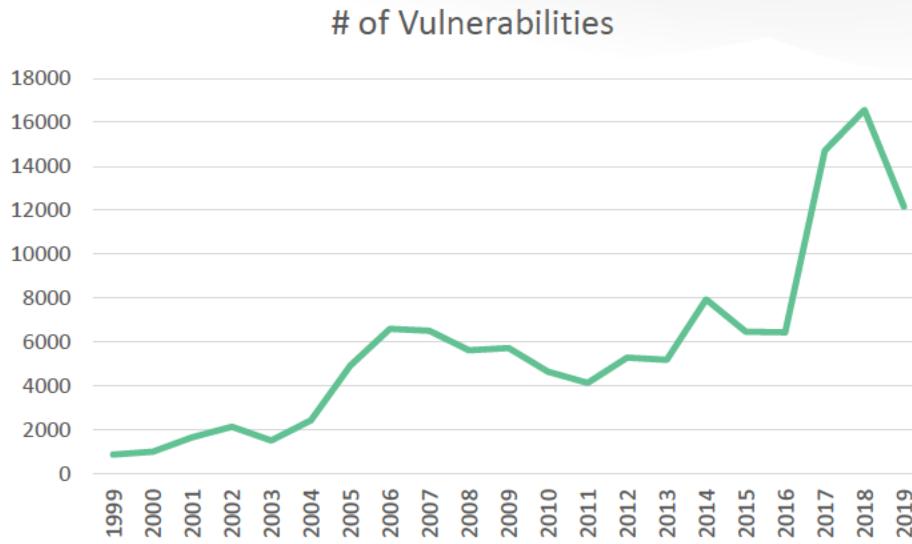
Next Find Vulns - NVD

The screenshot shows the NVD search interface. At the top, there's a navigation bar with the NIST logo, 'Information Technology Laboratory', and the 'NVD' logo. Below the navigation bar is a search form titled 'Search Vulnerability Database'. The search form includes fields for 'Search Type' (Basic or Advanced), 'CVSS Metrics' (Version 2.x or Version 3), 'Published Date Range', 'Last Modified Date Range', 'Contains Hyperlinks' (US-CERT Technical Alerts, US-CERT Vulnerability Notes, OVAL Queries), and various search filters like 'Results Type' (Overview or Statistics), 'Keyword Search', 'CVE Identifier', 'Category (CWE)', 'CFE Name', 'Vendor', and 'Product'. There are also dropdown menus for 'Category (CWE)' and 'CFE Name'. A note at the bottom states: 'NOTE: Only vulnerabilities that match ALL keywords will be returned. Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.'

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



Seems to be Working?



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

Component Issue



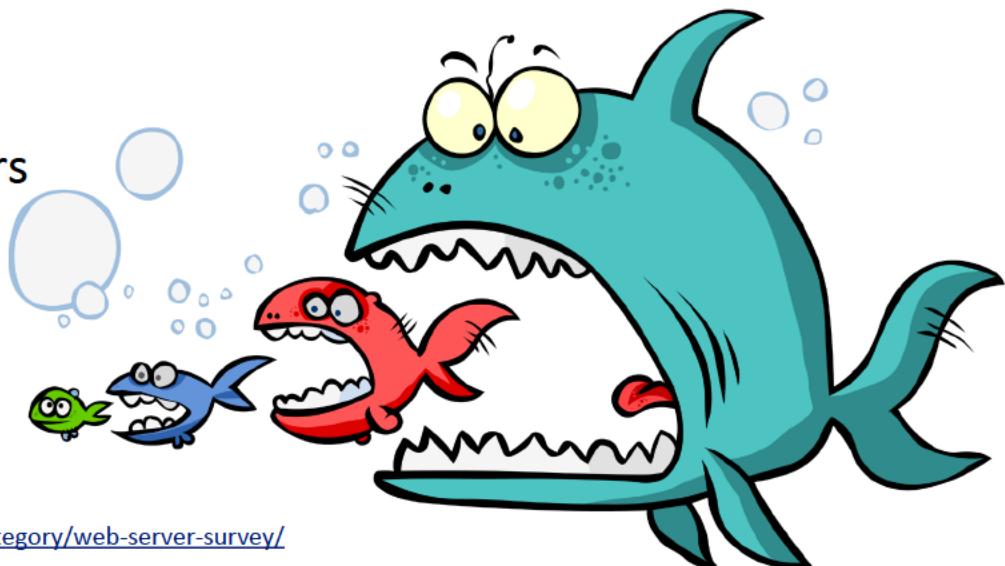
324 OpenSSL Vulns

3208 Products,
with SSL
as component

¹https://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 March¹
 - 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 NoSolved

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

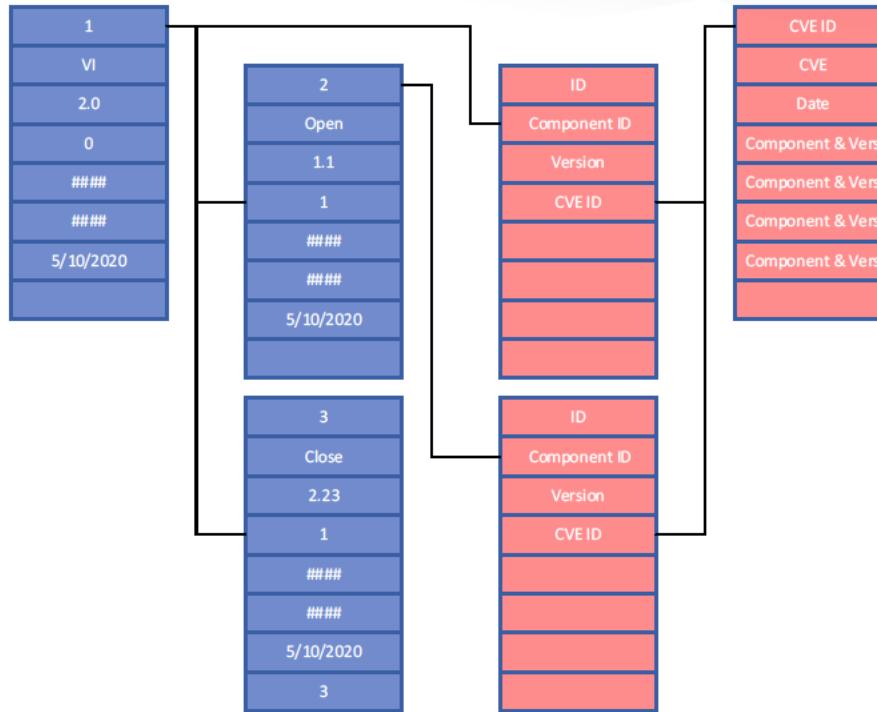
ID
Product
Version
Component of ID
SHA256
MD5
Date
Stuff

Product Table

CVE ID
CVE
Date
CVSS
Scores
Description
Component & Vers
Component & Vers

CVE Table

Relationships

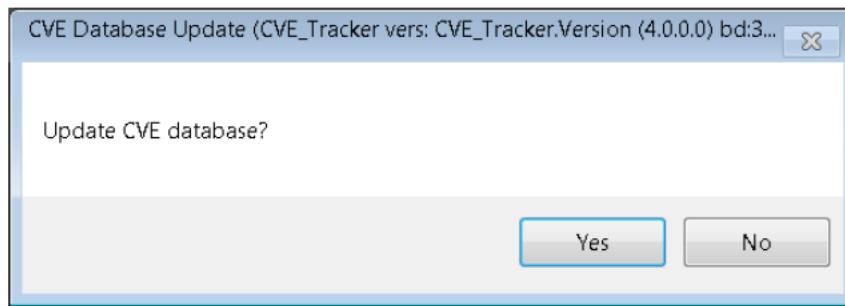


Procedurally

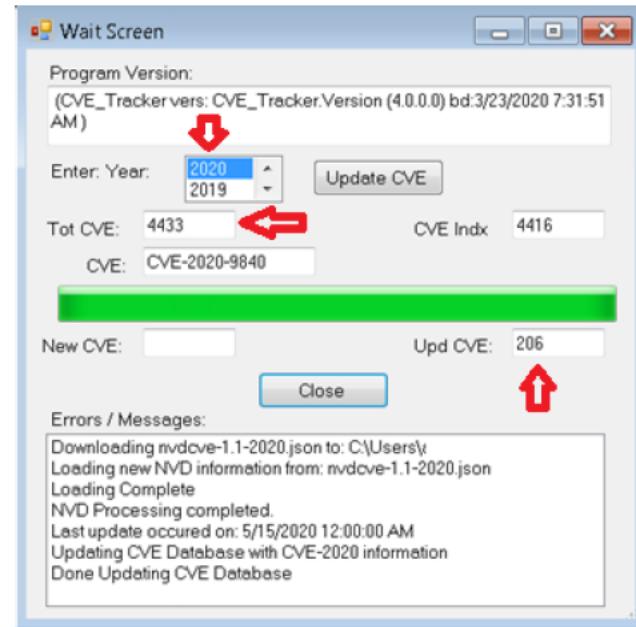
- Need to Load new CVEs daily
 - Need to review old products for new CVEs every day.
- Need to detect new products on systems.
 - Need to review new product against known CVEs.
- Need to notify ‘someone’ of:
 - New products & Components
 - CVEs associated with new products / components
- Provide triage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

Update the CVE List

Always Ask

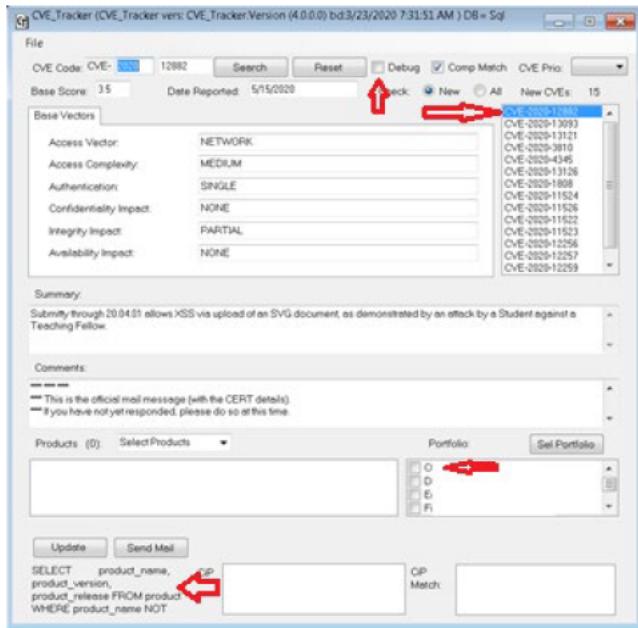


Download Screen



Thoughts

Top Screen



New Product List

This screenshot shows the 'New Product List' screen. At the top, there's a navigation bar with tabs: 'New', 'Test Daily', 'Product', 'New Prod', 'Add Vers', 'CVEs', 'General', 'Ck Prod', 'Ck Component', and 'SQL'. The 'New' tab is highlighted. Below the tabs, there are fields for 'Portfolio' and 'Product'. A 'LastRun:' field contains the date '2020-05-15'. To the right of this field are buttons for 'Update Date', 'Find', and 'Find All'. A checked checkbox labeled 'Check Date Since Last Run' is also present. The main area is a large grayed-out section labeled 'Version'. At the bottom, there's a table with columns 'Portfolio', 'Product', 'Version', and 'Date', and a 'Auto' button.

Next Step: Build a Proof of Concept

Daily Test

The screenshot shows a software interface for 'Daily Test'. At the top, there's a navigation bar with tabs: New, Test Daily, Product, New Prod, Add Vers, CVEs, General, Ck Prod, Ck Component, and SOL. Below the navigation bar, there are dropdown menus for 'Portfolio' and 'Product'. Under 'Versions', there are four buttons: 'Run All', 'Run Cur', 'Update', and 'eMail', each with a red arrow pointing to it. To the right of these buttons is another button labeled 'Next'. Below these buttons are two checkboxes: 'Auto' and 'New CVEs' (which is checked), and 'Ignore Errs'. A red arrow points to the 'Ignore Errs' checkbox. Further down, there are fields for 'Code' and 'Contacts', and buttons for 'Processing' (with a progress bar), 'Portfolio' (with a green bar), and 'Product'. There are also sections for 'Status' and 'Messages'. At the bottom, there are links for 'Add CVE', 'CVI Prx', 'CVE Component', 'Component & Version in our Product', and 'Tech Link'.

CVE List by Component

The screenshot shows a software interface for 'CVE List by Component'. At the top, there's a navigation bar with tabs: New, Test Daily, Product, New Prod, Add Vers, CVEs, General, Ck Prod, Ck Component, and SOL. Below the navigation bar, there's a search bar for 'CVE Component' and a 'Version' dropdown. To the right of the search bar is a 'Clear List' checkbox. Underneath, there are radio buttons for 'Search: Strict' and 'Fuzzy' (which is selected), with a red arrow pointing to it. A 'Find CVEs' button is next to the radio buttons. Below the search area is a table titled 'CVE List' with columns: CVE, CVSS, Date, Version, and Component. The table currently has no data.

Eventually...

list of components in products

Components CVEs, Products, Mach

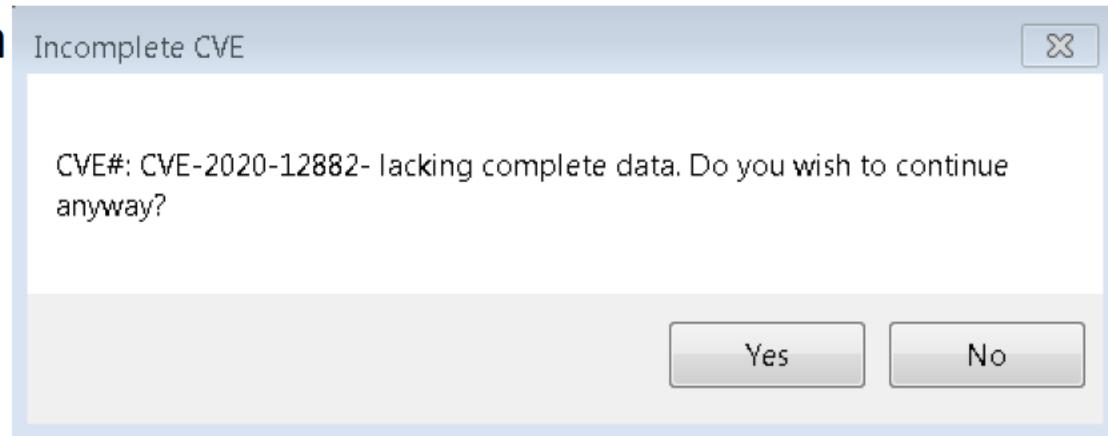
Product	Version	Released	Current Vers	Our Rel Date	Component	CVers	Contact

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 Information



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

RSA® Conference 2020 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**