Finding N-day Security Vulnerabilities in Third-party Software

Static Analysis Days @ Verifysoft, May 2021

Paul Anderson, VP of Engineering GrammaTech, Inc.

1

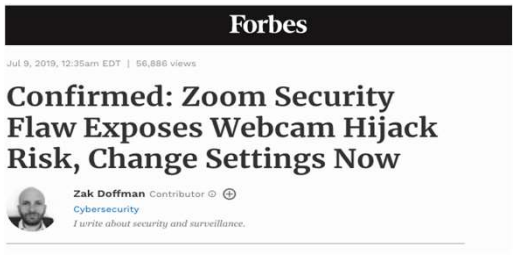
Outline

- N-day vulnerabilities
- Risks of third-party software
- Techniques for finding N-days
- N-days in Binaries

GRAMMATECH

2

COTS Vulnerabilities


Forbes

Jul 9, 2019, 12:35am EDT | 56,886 views

Confirmed: Zoom Security Flaw Exposes Webcam Hijack Risk, Change Settings Now

Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.


Forbes

EDITORS' PICK | Dec 23, 2019, 03:44am EST | 136,547 views

Windows 10 Security Warning As Dropbox Zero-Day Is Confirmed

Davey Winder Senior Contributor
Cybersecurity
I report and analyse breaking cybersecurity and privacy stories


The New York Times

rus Outbreak › | LIVE Latest Updates | Maps and Cases | See Your Local Risk | New Variants Tracker

Zoom's Security Woes Were No Secret to Business Partners Like Dropbox

Dropbox privately paid top hackers to find bugs in software by the videoconferencing company Zoom, then pressed it to fix them.

GRAMMATECH

COTS Vulnerabilities


ZDNet

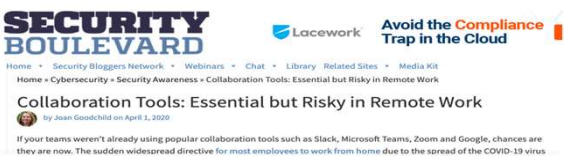
MUST READ: The global quantum computing race has begun. What will it take to win it?

Slack fixes vulnerability exploitable for session hijacking, account takeovers


Security Intelligence

Home / Threat Research / Malware

Killer Music: Hackers Exploit Media Player Vulnerabilities


SECURITY BOULEVARD

Lacework Avoid the Compliance Trap in the Cloud

Collaboration Tools: Essential but Risky in Remote Work

by Joan Goodchild on April 1, 2020

If your teams weren't already using popular collaboration tools such as Slack, Microsoft Teams, Zoom and Google, chances are they are now. The sudden widespread directive for most employees to work from home due to the spread of the COVID-19 virus


threatpost

Android Keyboard App Could Swindle 40M Users Out of Millions

Google Discloses Chrome Flaw Exploited in the Wild

Lindsey O'Donnell


threatpost

Brian Donohue On Security and Journalism

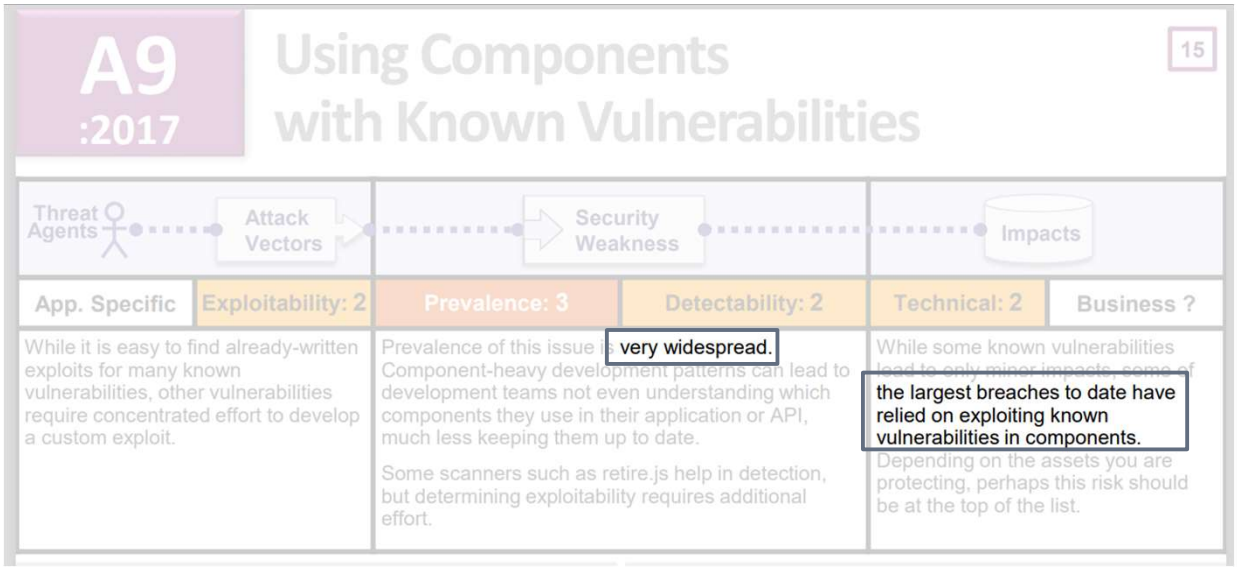
PeopleSoft Vulnerabilities Elevate ERP Security Issues

Michael Mimoso

ORACLE

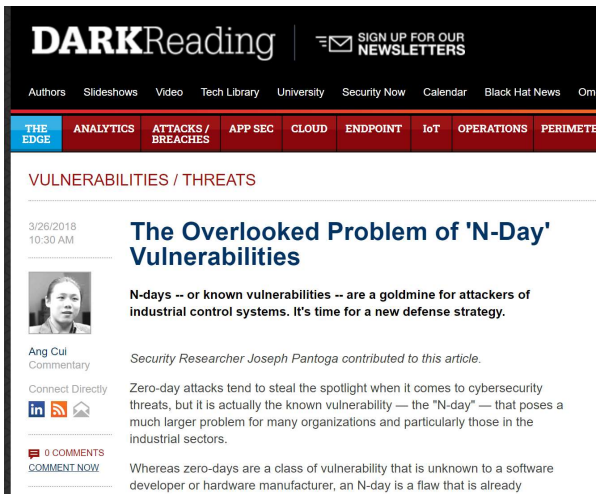
GRAMMATECH

OWASP Top 10



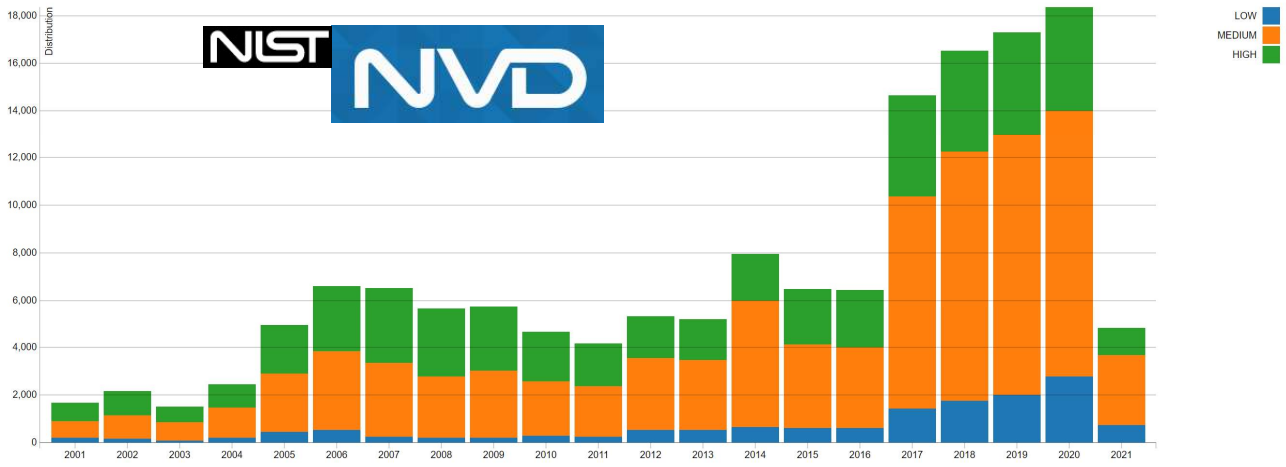
Definitions of Vulnerabilities

- 0-day
  - Just disclosed
  - No patch available
  - Exploits may not be widespread
- N-day
  - Patch *is* available
  - Exploits *likely* to be rampant in the wild



https://www.darkreading.com/vulnerabilities---threats/the-overlooked-problem-of-n-day-vulnerabilities/a/d-id/1331348

Trend: SW Increasingly Under Attack



Public n-day disclosures (with severity scores); snapshot taken April 13th 2021
https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

GRAMMATECH

N-days: a Major Threat

99.9% of exploited n-days disclosed over a year
Verizon DBIR 2015

Computer systems used by federal agencies often have n-days
U.S General Accountability Office (GAO) Report on Information Security, December 2018

Weapons systems rely on commercial and open-source software, and are subject to n-day exploits
U.S GAO Report on Weapon Systems Cybersecurity, October 2018

GRAMMATECH

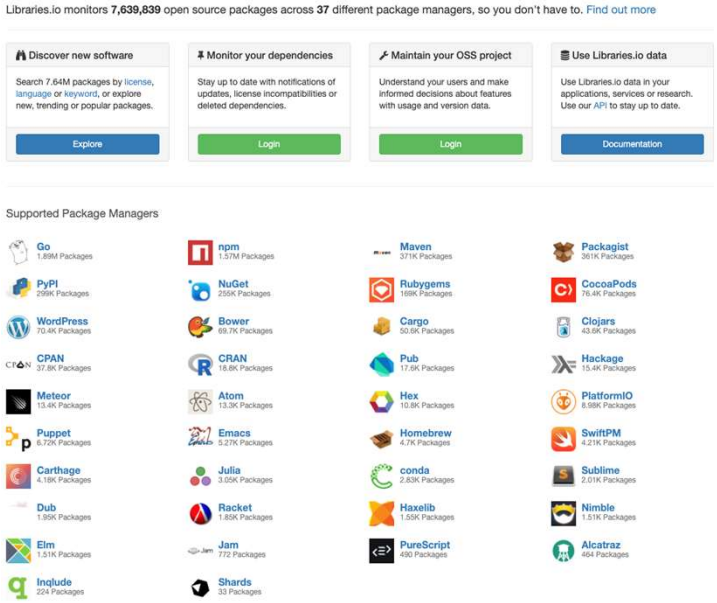
Equifax Data Breach, 2017

- Sensitive personal data of 148 Million Americans stolen
  - Including SSN
- Cost Equifax at least $380M (possibly up to $600M)
- Estimated cost to Americans (for freezing credit): $1.4B
- Exploited an n-day in the Java Struts framework
  - Left unpatched for several months (patch was publicly known)

Outline

- N-day vulnerabilities
- Risks of third-party software
- Techniques for finding N-days
- N-days in Binaries

OSS Is Integral to Modern Development

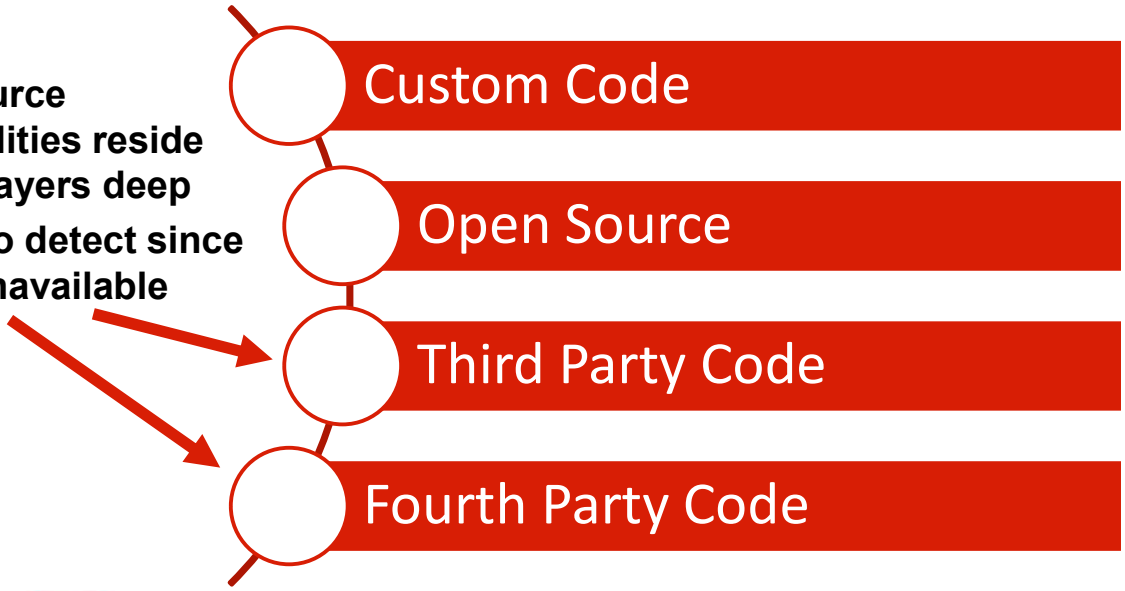


GRAMMATECH

Hidden Open Source Vulnerabilities

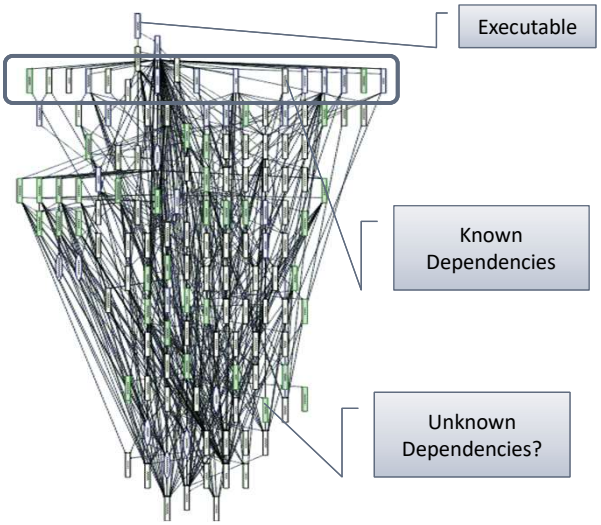
Open-Source vulnerabilities reside multiple layers deep

Difficult to detect since source unavailable



GRAMMATECH

Reality of Modern SW Development



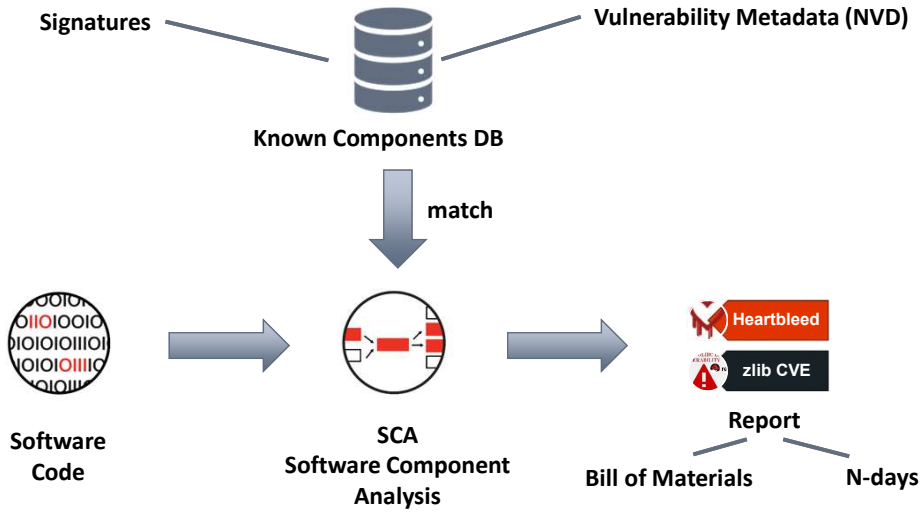
GRAMMATECH

Outline

- N-day vulnerabilities
- Risks of third-party software
- Techniques for finding N-days
- N-days in Binaries

GRAMMATECH

Software Component Analysis (SCA)



GRAMMATECH

Source vs Binary SCA

- Source-code SCA is well-established
  - Several commercial tools and services available
  - Techniques from Information Retrieval scale and work well
    - Hashing, Signature matching, n-grams, etc.
- Binary SCA is *hard*….

GRAMMATECH

Binary SCA Use Cases

Application Development - Internal and External Use

- Product Configurators
- Sales Forecasting
- Database applications
- Workflow applications
- Customer facing apps
- ERP

Product Development

PURESTORAGE, EMERSON, TESLA, NORTHROP GRUMMAN, Panasonic, DENSO

COTS Deployed Internally

zoom, Adobe, Office, slack, Dropbox

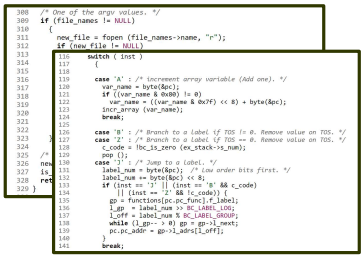
GRAMMATECH

Outline

- N-day vulnerabilities
- Risks of third-party software
- Techniques for finding N-days
- N-days in Binaries

GRAMMATECH

Why Binary SCA is Difficult



Source Code

Components:
- libxyz v2.3
- openABC v4.1.2

Unknown Transformations and Toolchains

Cut-and-paste
Forking and refactoring
Compilers
Linkers

Binary Code

What components?
What versions?

Critical Technical Challenge

Assembly listings for the Heartbleed bug, compiled using gcc-4.4 and clang-3.2:

tls1_process_heartbeat: gcc-4.4

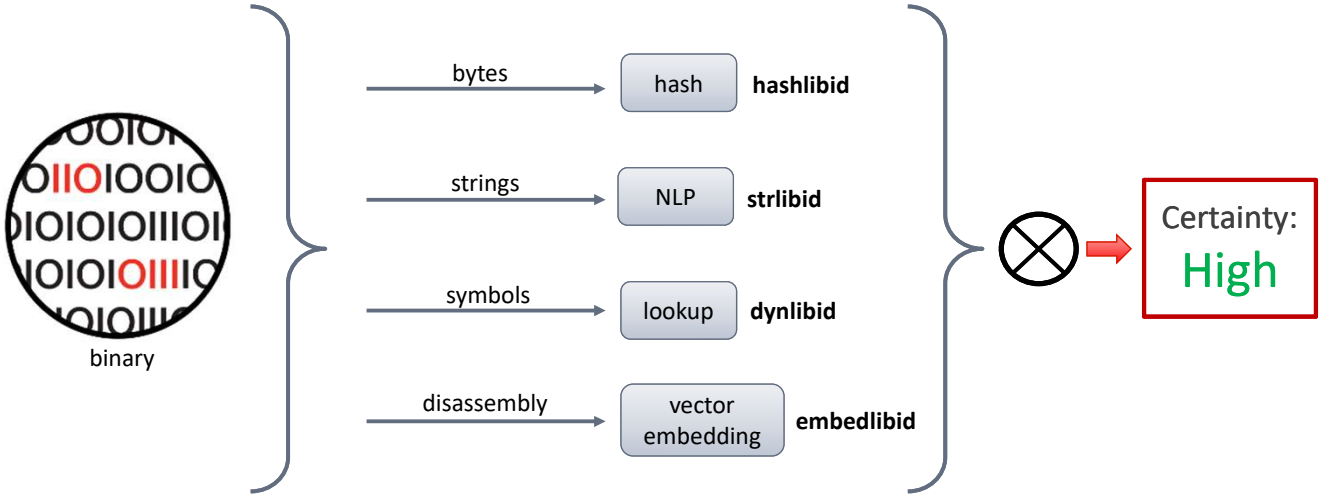
```
sub esp,0x4C
mov dword [esp+76+var_C],esi
mov esi,dword [esp+76+s]
mov dword [esp+76+var_10],ebx
mov dword [esp+76+var_8],edi
mov dword [esp+76+var_4],ebp
mov ecx,dword [esi+88]
call __i686.get_pc_thunk.bx
add ebx,0x2D6F1
mov ebp,dword [ecx+280]
movzx eax,byte [ebp]
mov word [esp+76+var_24],ax
movzx edx,byte [ebp+1]
movzx edi,byte [ebp+2]
shl edx,8
or edi,edx
...
```

tls1_process_heartbeat: clang-3.2

```
push ebp
push ebx
push edi
push esi
sub esp,0x2C
call loc_2B3EC
loc_2B3EC: pop ebx
add ebx,0x2660C
mov eax,dword [esp+60+arg_0]
mov ecx,dword [eax+88]
mov edi,dword [eax+100]
mov dword [esp+60+var_20],edi
mov ebp,dword [ecx+280]
movzx edx,byte [ebp+2]
mov dword [esp+60+var_14],edx
movzx esi,byte [ebp+1]
...
```

The same source code can look very different at the binary level

Approach: Biometrics for Components



GRAMMATECH

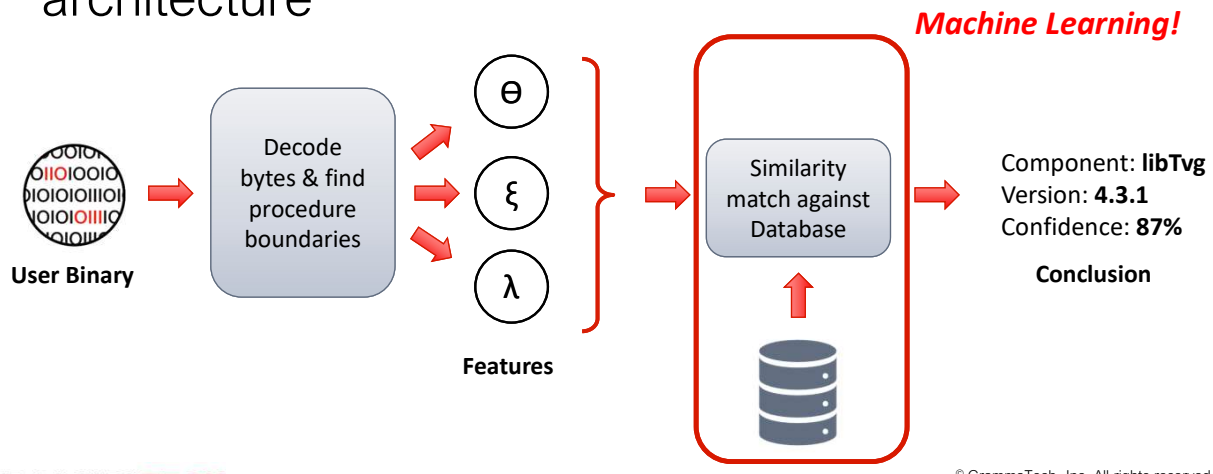
Superficial Properties of Binaries

- Properties are independent of the instruction set architecture
- Hashes
  - Compute hash of the file and look up in catalog of hashes
- Strings
  - Extract sequences of bytes that make up strings
- Symbols
  - Extract symbolic references

GRAMMATECH

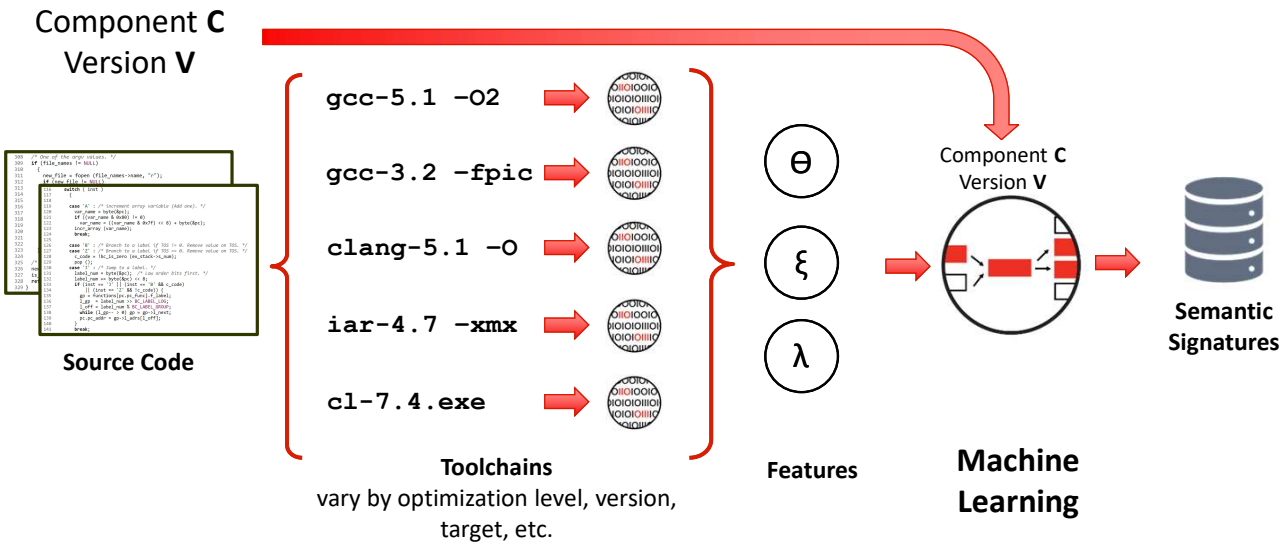
Deeper Properties of Binaries

- Properties sensitive to the instruction set architecture



GRAMMATECH

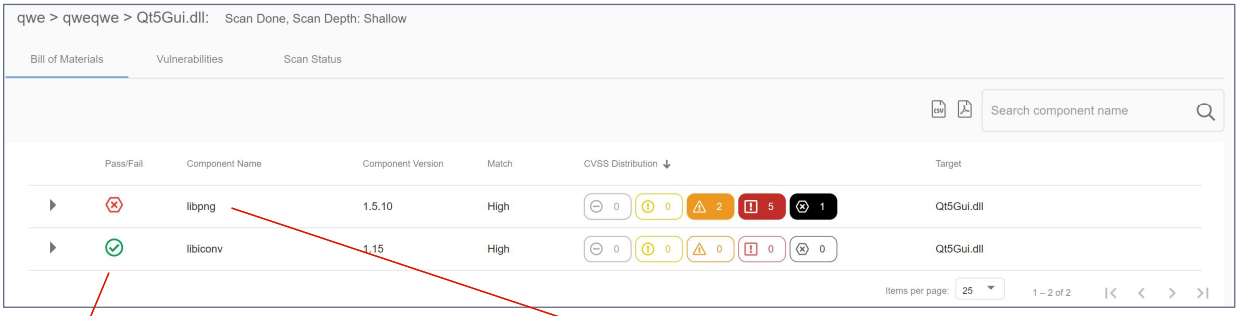
Machine Learning to Recognize Components



GRAMMATECH

Example: Bill of Materials

Scan of a single file: Qt5Gui.dll

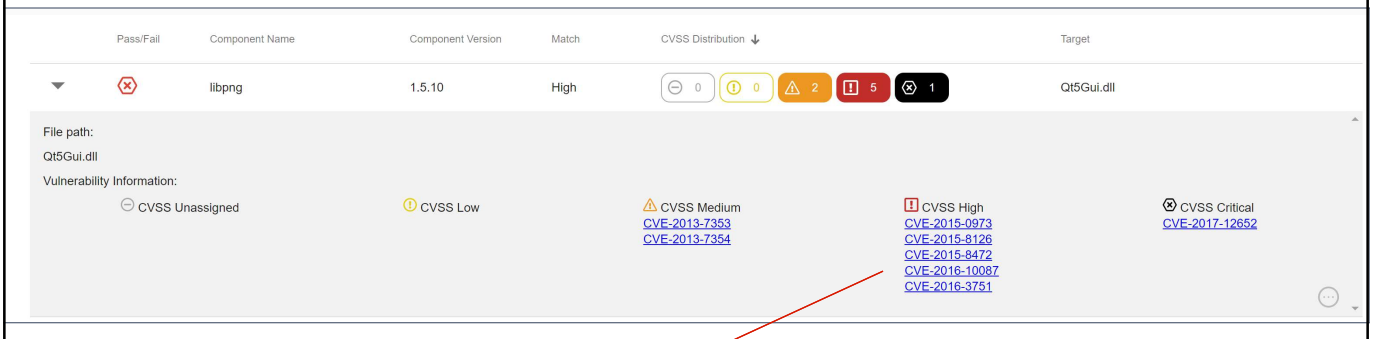


libiconv detected, but safe

libpng detected, with several vulnerabilities

GRAMMATECH

Example: Vulnerabilities View



Link to CVEs associated with the detected version of *libpng*

GRAMMATECH

Conclusion

- N-day vulnerabilities are abundant
- Particularly pernicious for Supply Chain Risk Management
- Software Composition Analysis tools can help close the door on large classes of serious security weaknesses
- Tools capable of analyzing binaries are now available