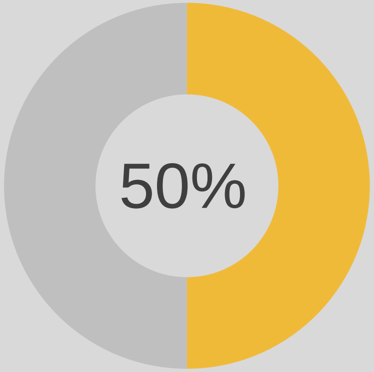
BLACKDUCK

SECURITY IN THE AGE OF OPEN SOURCE

February 19, 2016

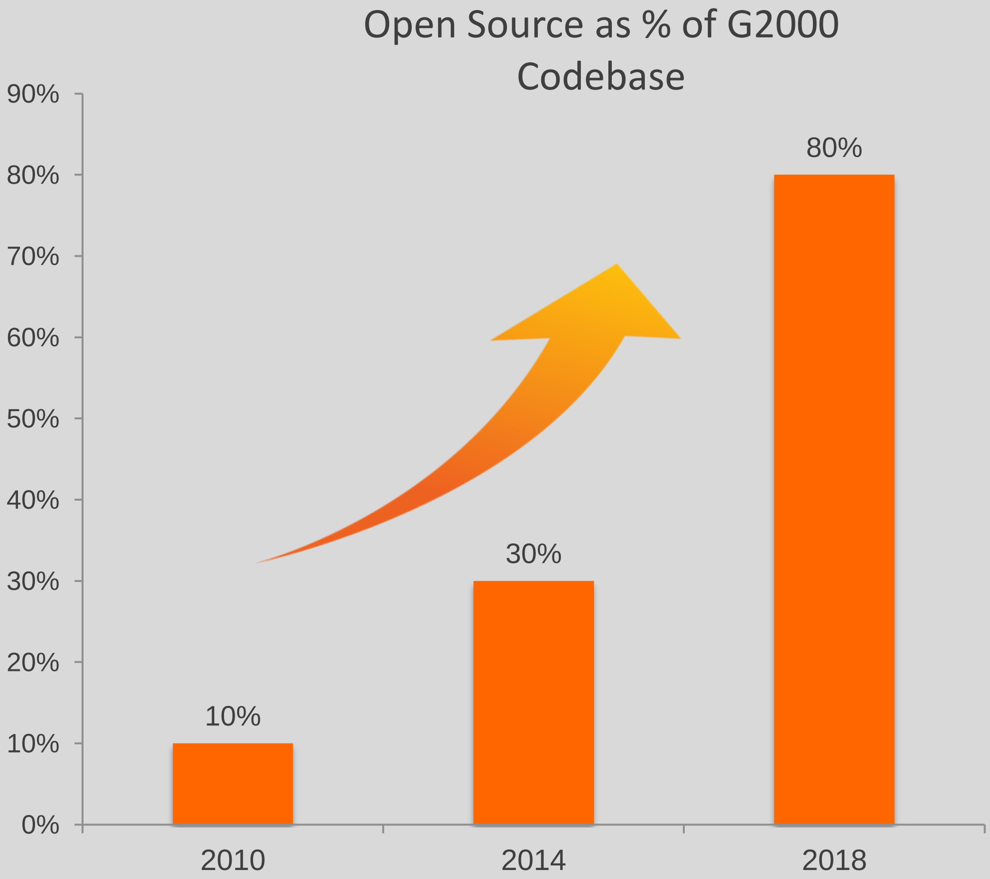
OPEN SOURCE HAS PASSED THE TIPPING POINT

"By 2016, Open Source Software will be included in mission-critical applications within 99% of Global 2000 enterprises."



Will face problems because of no policy.

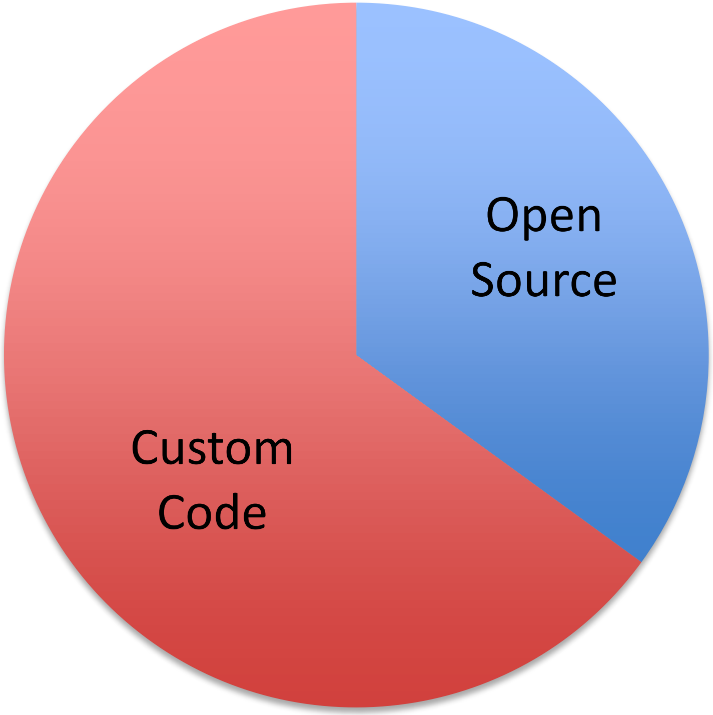
Gartner



Reference: Gartner, Inc.

HOW PERVASIVE IS OPEN SOURCE?

Composition of software tested across 1400 Black Duck customers



>98% of the applications tested used open source

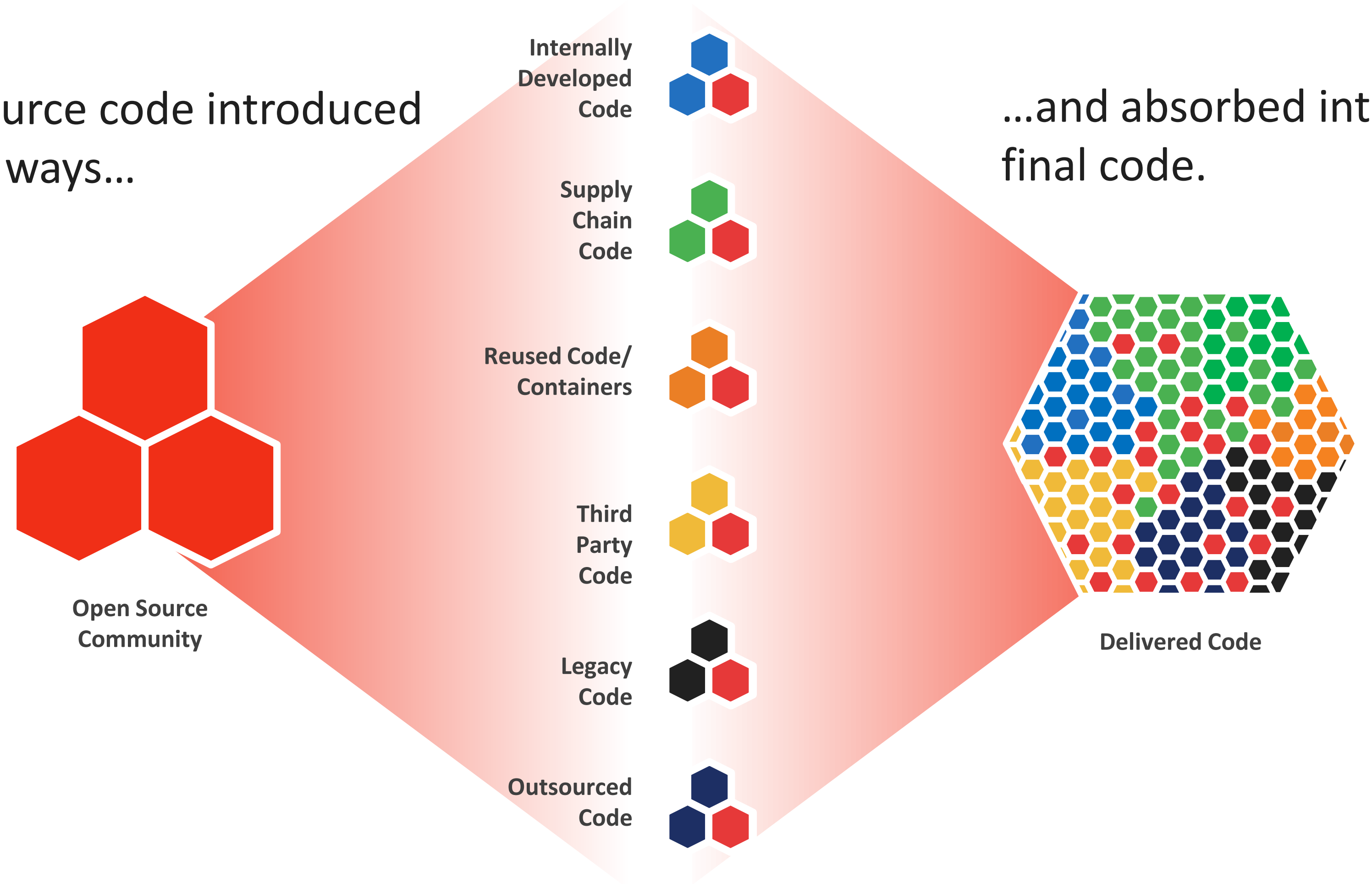
On average, open source comprised over 30% of the code base

Reference: Black Duck Software audits

HOW OPEN SOURCE ENTERS A CODEBASE

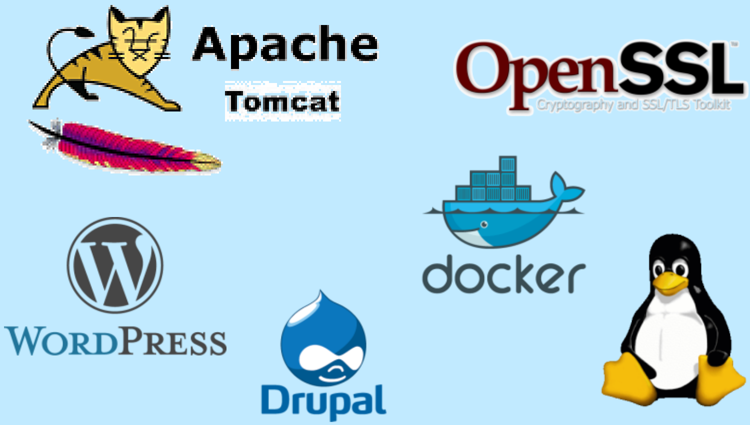
Open source code introduced in many ways…

…and absorbed into final code.



OPEN SOURCE: EASY TARGETS

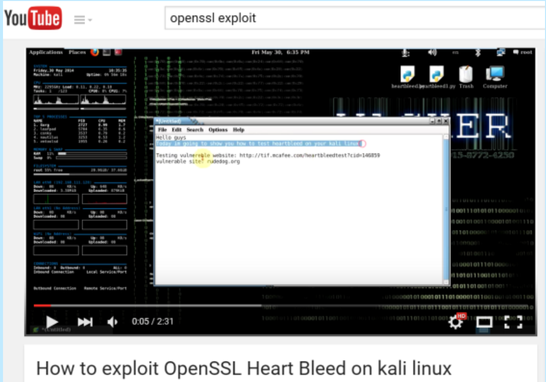
Used everywhere



Easy access to code

Vulnerabilities are publicized

Exploits readily available

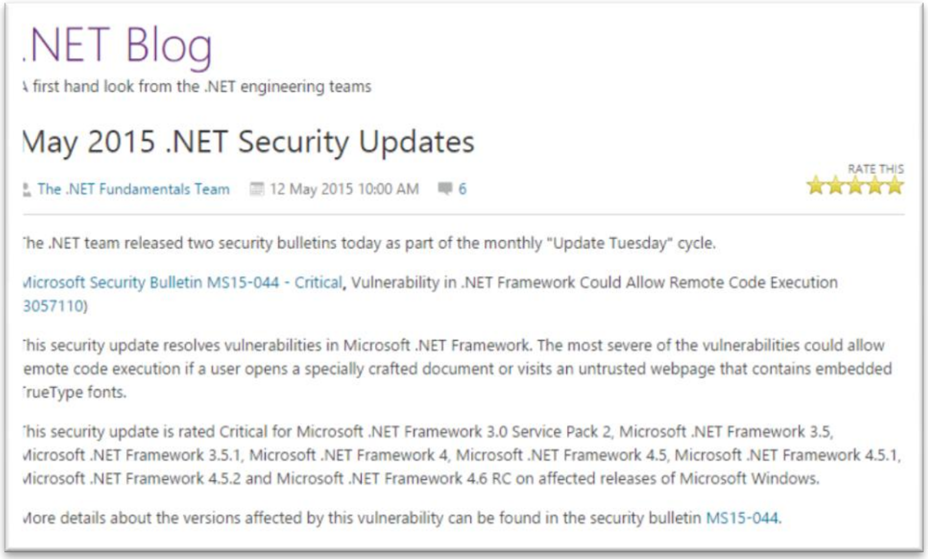


```
Hello guys
Today im going to show you how to test heartbleed on your kali linux

Testing vulnerable website: http://tif.mcafee.com/heartbleedtest?cid=146859
vulnerable site: rudedog.org
```

How to exploit OpenSSL Heart Bleed on kali linux

WHO'S RESPONSIBLE FOR SECURITY?

Commercial Code



.NET Blog

A first hand look from the .NET engineering teams

May 2015 .NET Security Updates

The .NET Fundamentals Team 12 May 2015 10:00 AM 6 RATE THIS ★★★★★

The .NET team released two security bulletins today as part of the monthly "Update Tuesday" cycle.

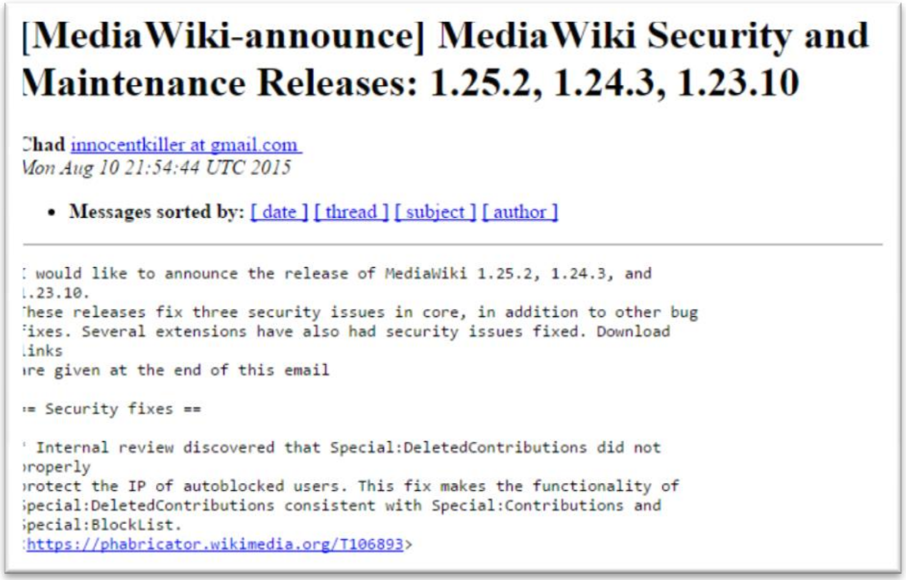
Microsoft Security Bulletin MS15-044 - Critical, Vulnerability in .NET Framework Could Allow Remote Code Execution (3057110)

This security update resolves vulnerabilities in Microsoft .NET Framework. The most severe of the vulnerabilities could allow emote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded TrueType fonts.

This security update is rated Critical for Microsoft .NET Framework 3.0 Service Pack 2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4, Microsoft .NET Framework 4.5, Microsoft .NET Framework 4.5.1, Microsoft .NET Framework 4.5.2 and Microsoft .NET Framework 4.6 RC on affected releases of Microsoft Windows.

More details about the versions affected by this vulnerability can be found in the security bulletin MS15-044.

Open Source Code



[MediaWiki-announce] MediaWiki Security and Maintenance Releases: 1.25.2, 1.24.3, 1.23.10

Chad innocentkiller at gmail.com
Mon Aug 10 21:54:44 UTC 2015

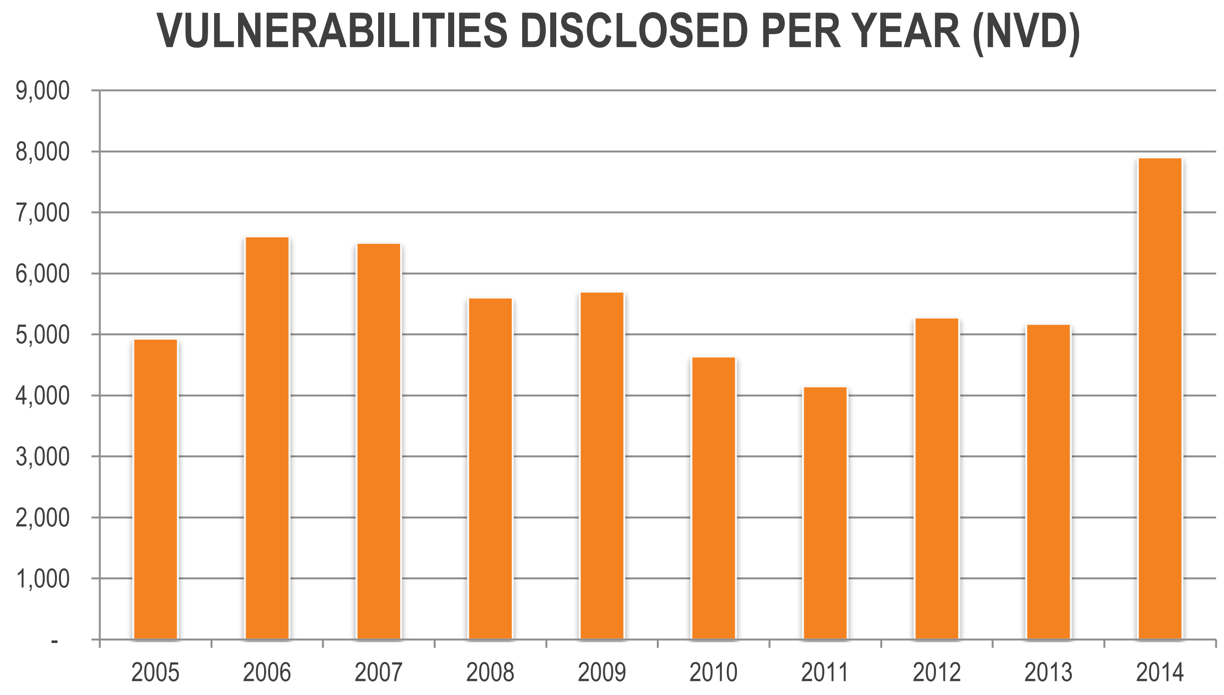
- **Messages sorted by:** [date] [thread] [subject] [author]

```
I would like to announce the release of MediaWiki 1.25.2, 1.24.3, and
1.23.10.
These releases fix three security issues in core, in addition to other bug
fixes. Several extensions have also had security issues fixed. Download
links
are given at the end of this email

== Security fixes ==

* Internal review discovered that Special:DeletedContributions did not
properly
protect the IP of autoblocked users. This fix makes the functionality of
Special:DeletedContributions consistent with Special:Contributions and
Special:BlockList.
<https://phabricator.wikimedia.org/T106893>
```

- Dedicated security researchers
- Alerting and notification infrastructure
- Regular patch updates
- **Dedicated support team with SLA**

- "community"-based code analysis
- Monitor newsfeeds yourself
- No standard patching mechanism
- **Ultimately, you are responsible**

NUMBER OF VULNERABILITIES ARE NOT DECREASING

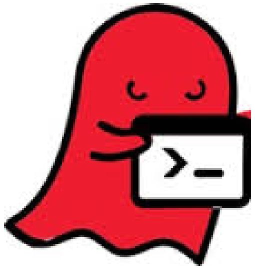


In 2014:

- Over 7,900 new vulnerabilities disclosed
- ~4,300 in Open Source, ~3,600 in commercial software

Reference: Black Duck Software knowledgebase, NVD

WHAT DO THESE VULNERABILITIES HAVE IN COMMON?



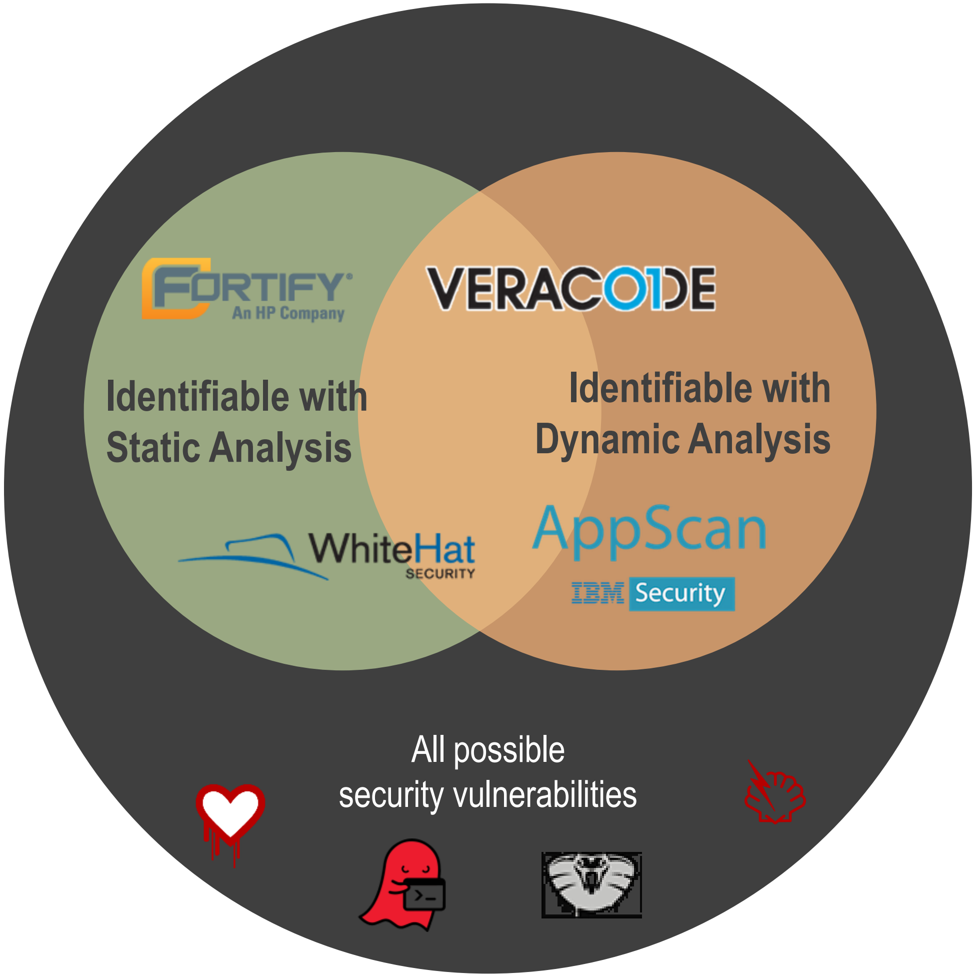
	Heartbleed	Shellshock	Freak	Ghost	Venom
Since:	2011	1989	1990’s	2000	2004
Discovered:	2014	2014	2015	2015	2015
Discovered by:	Riku, Antti, Matti, Mehta	Chazelas	Beurdouche	Qualys researchers	Geffner
Component:	OpenSSL	Bash	OpenSSL	GNU C library	QEMU

AUTOMATED TOOLS MISS MOST OPEN SOURCE VULNS

- SAST and DAST only discover common vulnerabilities

- Undiscovered vulnerabilities are too complex, nuanced

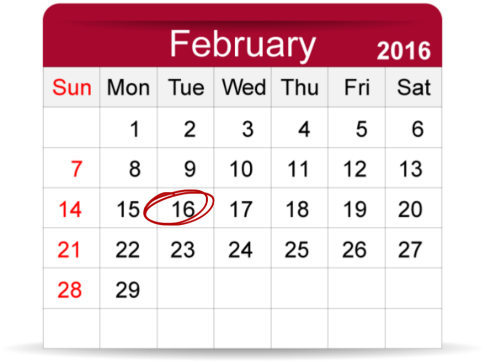
- 4,000+ disclosed in 2014, <1% found by automated tools


FORTIFY An HP Company
VERACODE
Identifiable with Static Analysis
Identifiable with Dynamic Analysis
WhiteHat SECURITY
AppScan
IBM Security
All possible security vulnerabilities

RECENT INCIDENT RESPONSE EXAMPLE

February 16, 2016:

Google discloses critical vulnerability in the GNU C Library, found in most Linux distributions and used by most Linux applications written in C and C++.

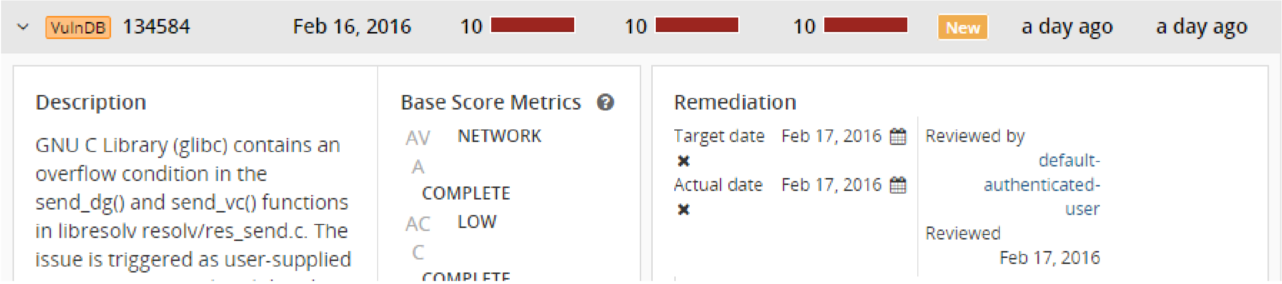


February 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29					

Same day:

Black Duck customers were alerted via VulnDB…



VulnDB 134584 Feb 16, 2016 10 10 10 New a day ago a day ago

Description

GNU C Library (glibc) contains an overflow condition in the send_dg() and send_vc() functions in libresolv resolv/res_send.c. The issue is triggered as user-supplied

Base Score Metrics

AV NETWORK
A COMPLETE
AC LOW
C COMPLETE

Remediation

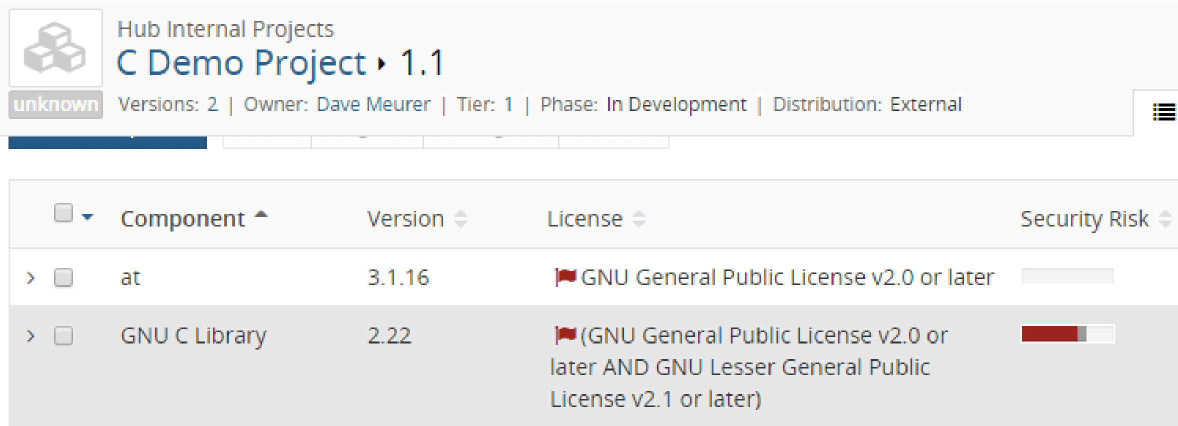
Target date Feb 17, 2016 ✖

Actual date Feb 17, 2016 ✖

Reviewed by default-authenticated-user

Reviewed Feb 17, 2016

…and knew which applications contained the vulnerability.



Hub Internal Projects

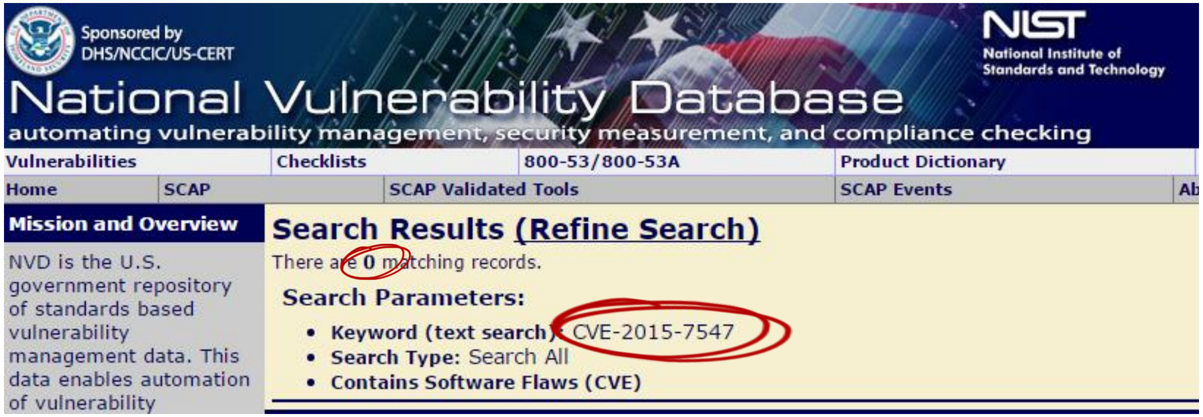
C Demo Project ▸ 1.1

unknown Versions: 2 | Owner: Dave Meurer | Tier: 1 | Phase: In Development | Distribution: External

□	Component	Version	License	Security Risk
□	at	3.1.16	GNU General Public License v2.0 or later	
□	GNU C Library	2.22	(GNU General Public License v2.0 or later AND GNU Lesser General Public License v2.1 or later)	🟥

INCIDENT RESPONSE EXAMPLE, CONT'D

2 days later, still no record in the NVD:



Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Home
SCAP
SCAP Validated Tools
SCAP Events
Ab
Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability

Search Results (Refine Search)

There are 0 matching records.

Search Parameters:

- **Keyword (text search):** CVE-2015-7547
- **Search Type:** Search All
- **Contains Software Flaws (CVE)**

➢ Was it discovered by SAST/DAST tools?
No, too complex for automated discovery.

➢ Could other OSS management tools find it?
No, because they depend on the NVD, which is generally weeks behind in processing new vulnerabilities.

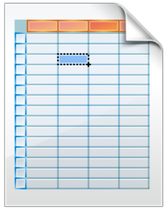
HOW ARE COMPANIES ADDRESSING THIS TODAY? NOT WELL.

Manual tabulation

- High effort
- Low accuracy

Spreadsheet-based inventory

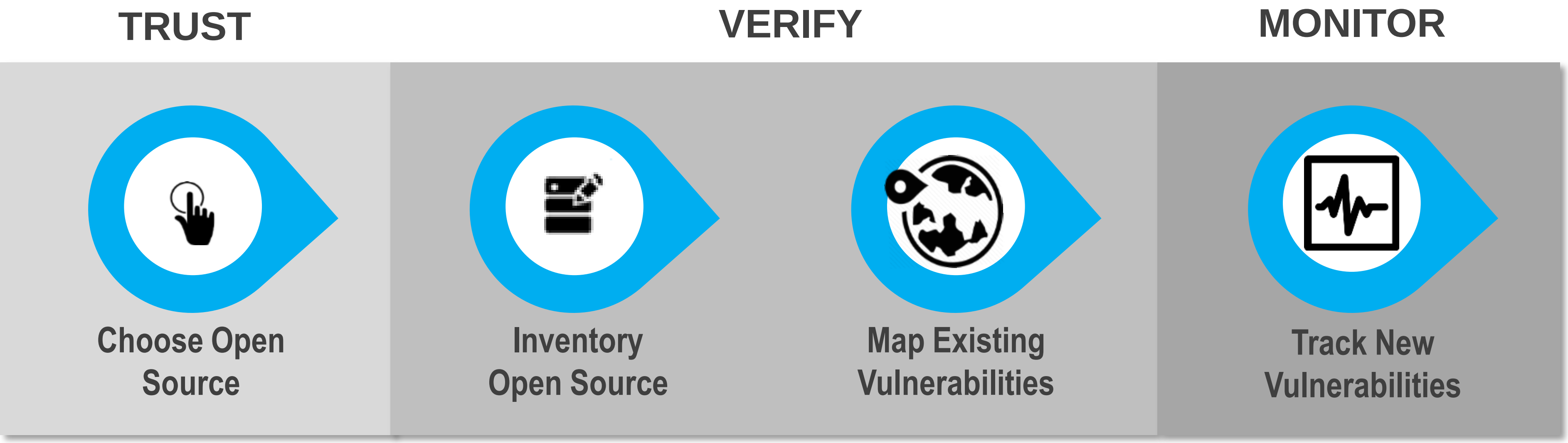
- Difficult maintenance
- Not source of truth



Tracking vulnerabilities

- Unmanageable (11/day)
- Labor intensive: match applications, versions, components, vulns

A SOLUTION TO SOLVING THIS PROBLEM WOULD INCLUDE THESE COMPONENTS



TRUST

VERIFY

MONITOR

Choose Open Source

Inventory Open Source

Map Existing Vulnerabilities

Track New Vulnerabilities

Proactively choose secure, supported open source

Maintain accurate list of open source components throughout the SDL

Identify vulns during development

Alert new vulns in production apps

BLACK DUCK CREATED AN INDUSTRY

24
Countries

185+
Employees

1,600
Customers

27 of the Fortune 100

7 of the top 10 Software companies, and 44% of the top 100

6 of the top 8 Mobile handset vendors

6 of the top 10 Investment Banks

Four Years in the “Software 500” Largest Software Companies

Six Years in a row for Innovation

Gartner Group “Cool Vendor”

Award for Innovation

Ranked #38 out of 500 Security Companies

NEXT STEPS

Let’s go speak with your head of application development and find out:

- What policies exist?
- Is there a list of components?
- How are they creating the list?
- Are they tracking vulnerabilities?
- How do they ensure nothing gets through?

BLACKDUCK

The Intelligent Management of Open Source