Attacking IoT Developers

Dr. Olaf Flebbe
of ät oflebbe.de

About me

PhD in computational physics

Doing Opensource for over 25 years:
Math libs for: Minix/gcc 68k, Linux libm.so.5,
ported perl and python to psion/epoc,
contributed to flightgear port to Windows/
Mac, Maintainer of msktutil

PMC of Apache Bigtop,
ASF Member

Backend Software Architect Bosch eBike

Attacking a ~~Big Data~~ IoT Developer

Dr. Olaf Flebbe
of ät oflebbe.de

ApacheCon Bigdata Europe

Aftermath: Attacking Big Data Developer

- codehaus.org now hosted by Apache

Security

- The Internet is not a safe place any more
- Attackers are using increasingly complex attacks in order to penetrate enterprises
- There is no well established awareness for:

Developer Attack Vector

- Any user of an insecure build process may download software artifacts which may penetrate himself or his customer
  - Investigate
  - Upstream fixes
  - Watch community to iron things out

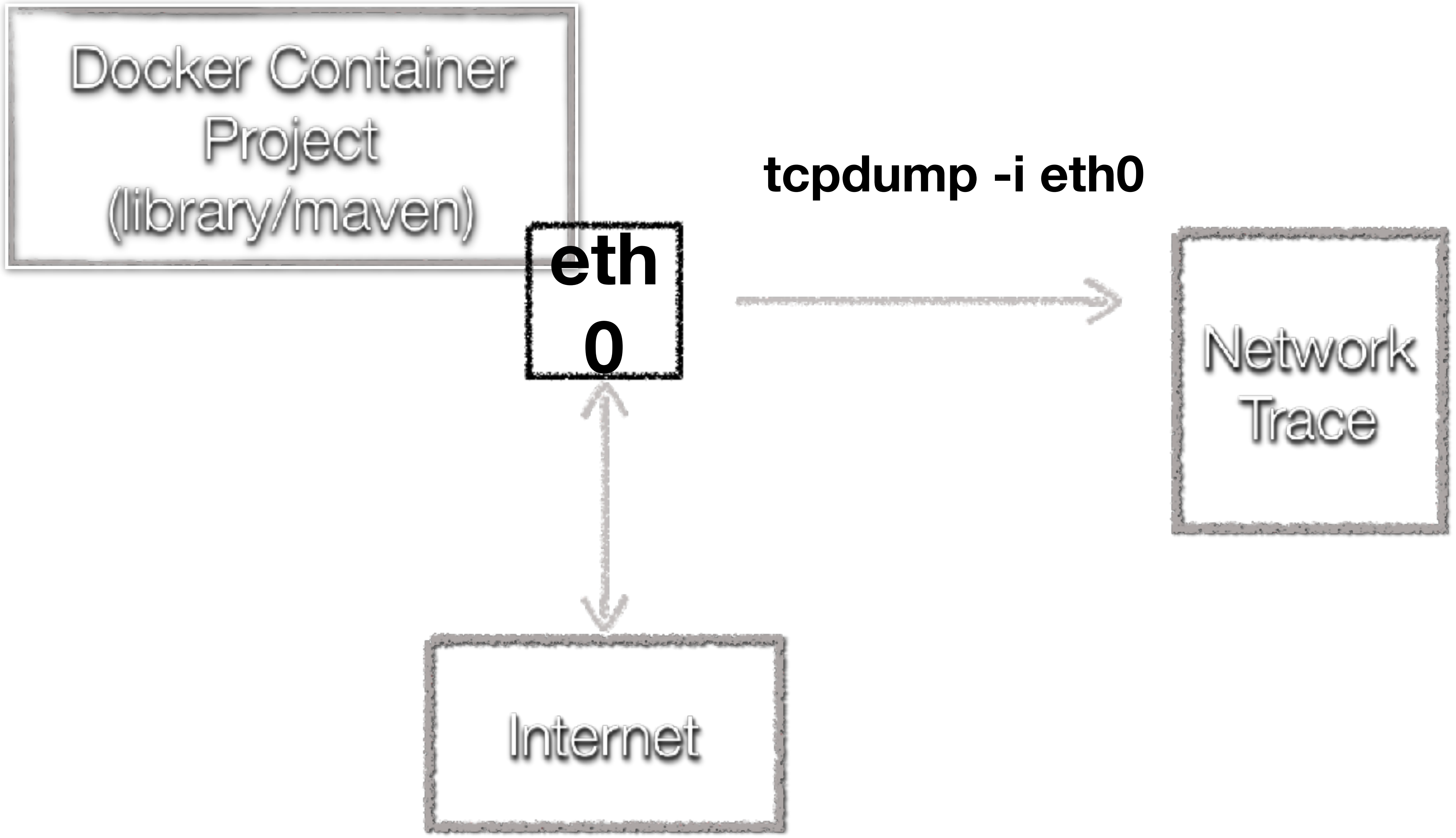
Method 1: Network analysis

- Catching complete network traffic while compiling codebase
- Create in depth package analysis of the traffic with an sophisticated network security monitor
- ...
- Profit

Toolset

Docker

- Clean Room, network separation
- Apache Maven images from dockerhub library
  - apt-get update && apt-get install tcpdump
  - tcpdump -i eth0 -s 0 -w /FILE &
  - mvn (-DskipTests) package
  - stop tcpdump
- docker cp container:/FILE .



Docker Container Project (library/maven)

eth
0

tcpdump -i eth0

Network Trace

Internet

Bro

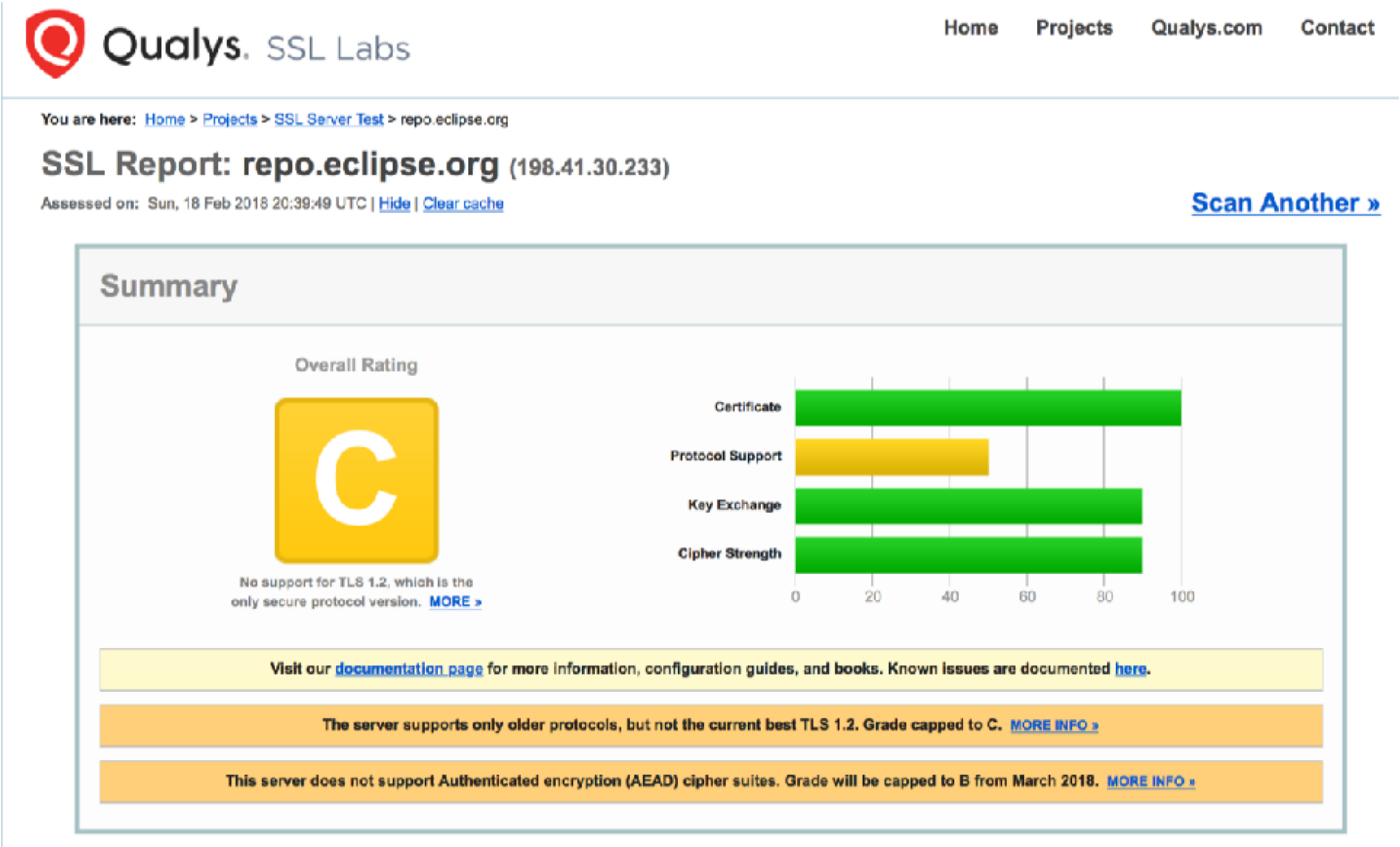
- Bro: The Network Security Monitor
- www.bro.org
  - Flexible, High performance, Stateful in depth Analysis
  - Analyse HTTP, HTTPS Certificate Chains, Fingerprinting of Downloads, Analyse DNS Requests and Answers
- blacktop/bro docker image
  - `docker run --rm -v $(pwd):/pcap  blacktop/bro -C -r FILE`

Watch out for:

- plain http traffic
- SSL Servers
- DNS queries
- Unidentified TCP packages

Repo issues

#1 eclipse



Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > repo.eclipse.org

SSL Report: repo.eclipse.org (198.41.30.233)

Assessed on: Sun, 18 Feb 2018 20:39:49 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

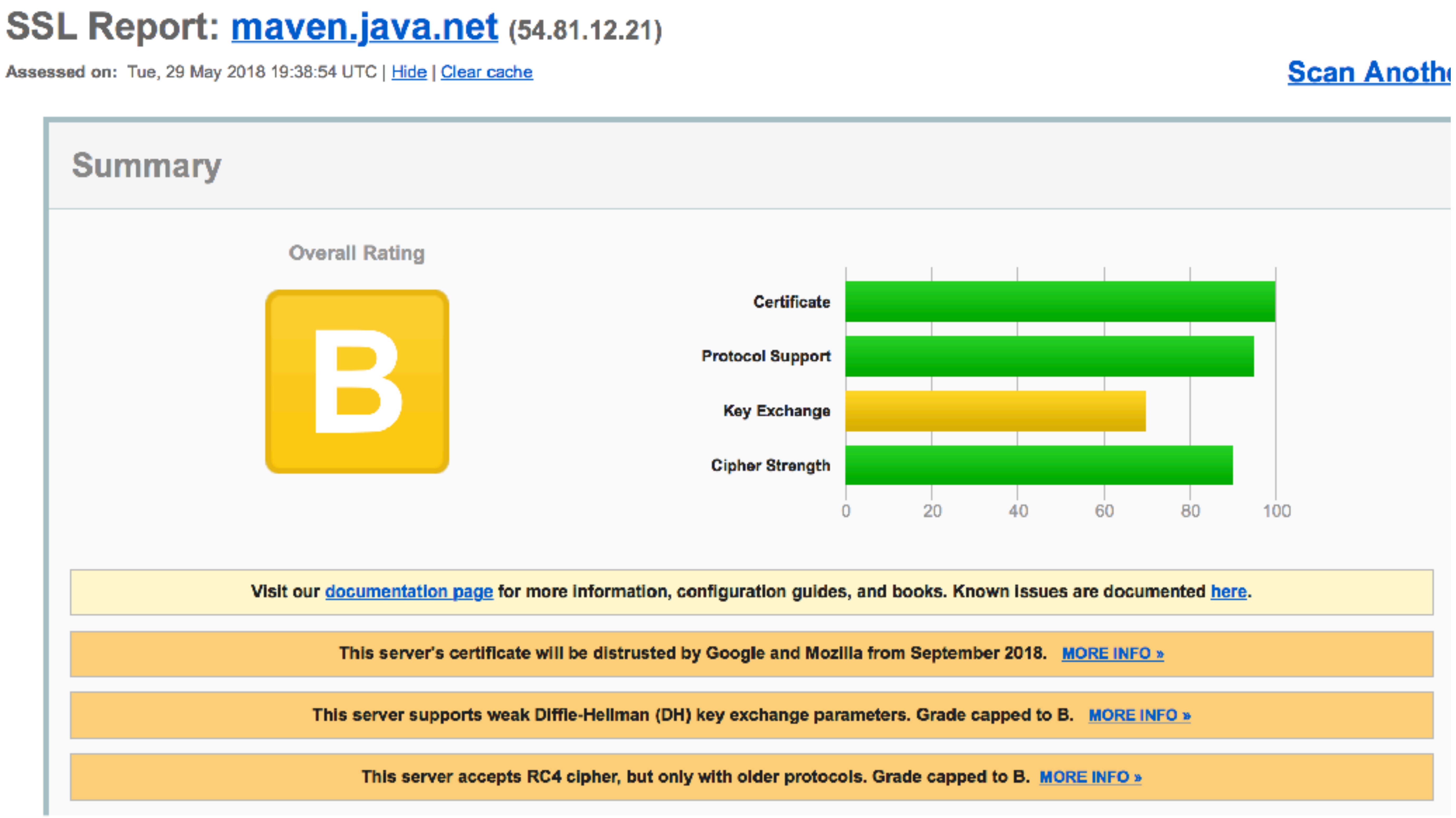
This server does not support Authenticated encryption (AEAD) cipher suites. Grade will be capped to B from March 2018. MORE INFO »

repo.eclipse.org

- Reported it on Feb 18th to security@eclipse.org: No reaction.
- Aggravated that maven central will only accept TLS 1.2 in 3 days
(15th of June, see sonatype blog)
- Asked Ralph Müller (German eclipse Representative) for comment:
- Eclipse is already working on it #515595, new reverse proxy soon in place for repo.eclipse.org

#2 maven.java.net

- According to ssllabs maven.java.net uses one of the old symantec certificate. Mozilla and Google distrusting them in Sep. because of repeated issues of symantec certificate practice.



SSL Report: maven.java.net (54.81.12.21)

Assessed on: Tue, 29 May 2018 19:38:54 UTC | Hide | Clear cache

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

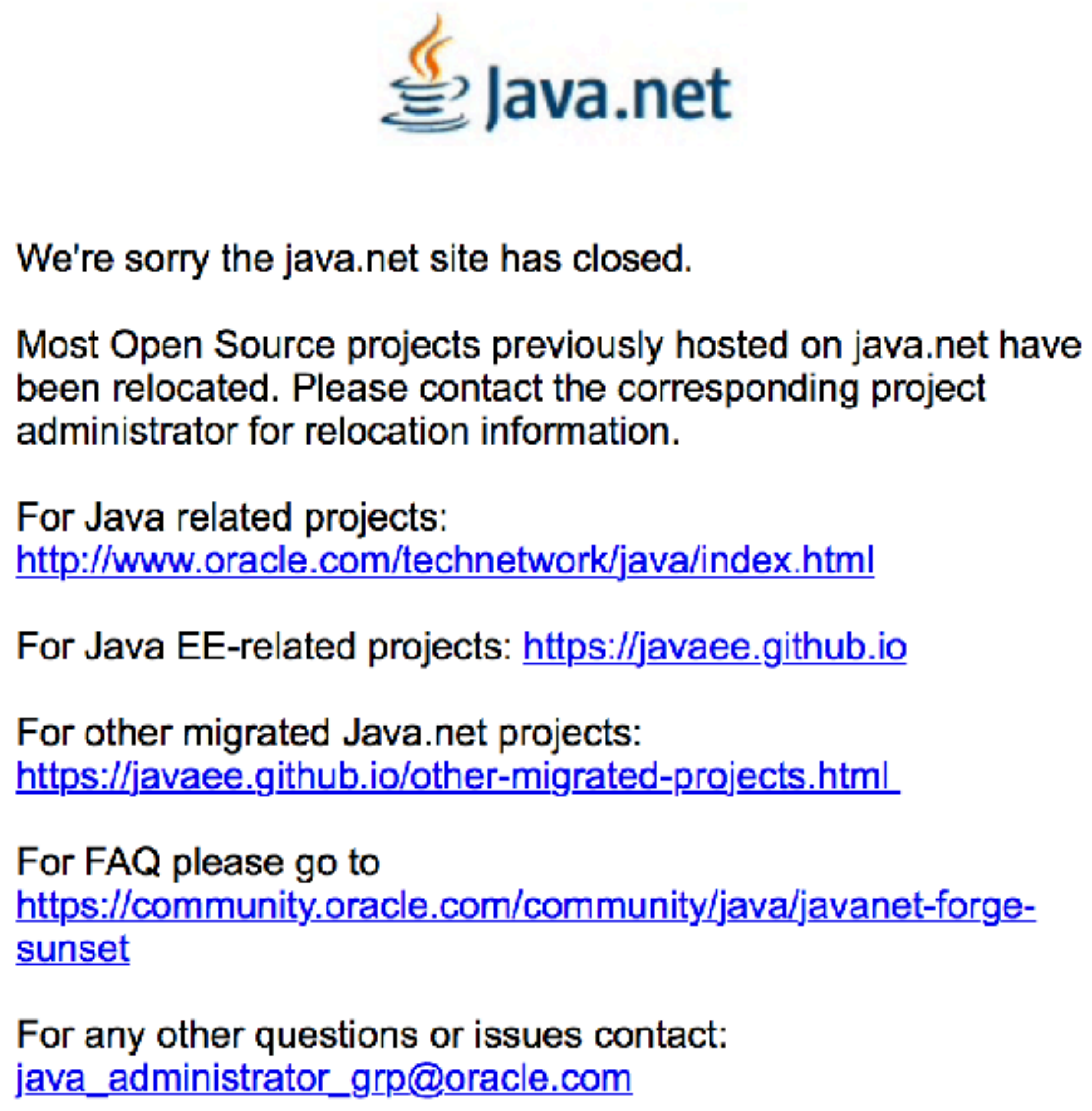
This server's certificate will be distrusted by Google and Mozilla from September 2018. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

Will java follow google?

- Will java/openjdk/oracle follow Google and mozilla
  Yes: java.maven.net will be broken.
- Still time to fix...
- I bet it will break openjdk-7/8 on Debian, if they dont renew.
- Asking for comment on Jun 5th: No answer so far.



We're sorry the java.net site has closed.

Most Open Source projects previously hosted on java.net have been relocated. Please contact the corresponding project administrator for relocation information.

For Java related projects:
http://www.oracle.com/technetwork/java/index.html

For Java EE-related projects: https://javaee.github.io

For other migrated Java.net projects:
https://javaee.github.io/other-migrated-projects.html

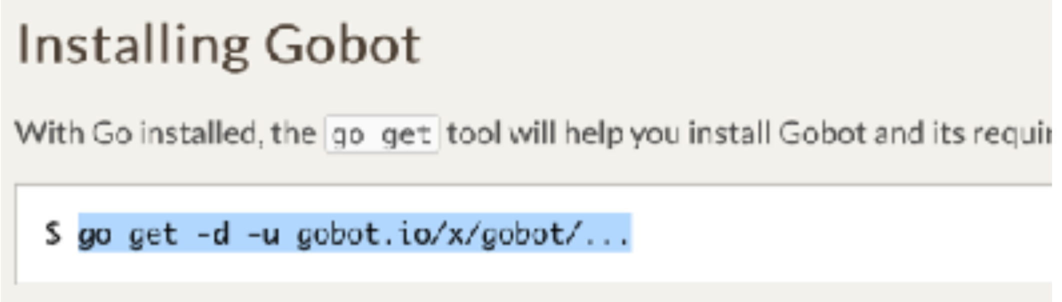
For FAQ please go to
https://community.oracle.com/community/java/javanet-forge-sunset

For any other questions or issues contact:
java_administrator_grp@oracle.com

Go(bot) repos

- Let's look at gobot.org
- go framework for robots
- go get (depency resolution) is designed with security in mind
- What possibly can go wrong?

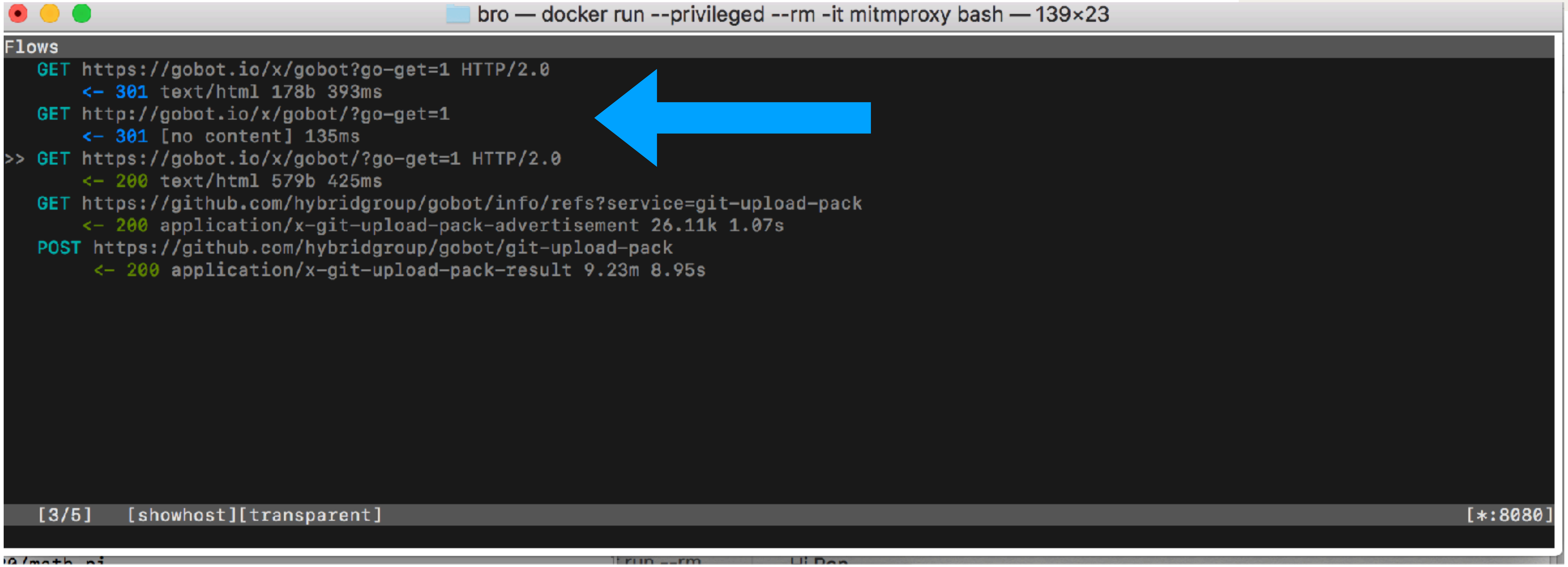
Triggered bro!
Investigated with mitmproxy



Installing Gobot

With Go installed, the `go get` tool will help you install Gobot and its requi

```
$ go get -d -u gobot.io/x/gobot/...
```



bro — docker run --privileged --rm -it mitmproxy bash — 139×23

```
Flows
   GET https://gobot.io/x/gobot?go-get=1 HTTP/2.0
       <- 301 text/html 178b 393ms
   GET http://gobot.io/x/gobot/?go-get=1
       <- 301 [no content] 135ms
>> GET https://gobot.io/x/gobot/?go-get=1 HTTP/2.0
       <- 200 text/html 579b 425ms
   GET https://github.com/hybridgroup/gobot/info/refs?service=git-upload-pack
       <- 200 application/x-git-upload-pack-advertisement 26.11k 1.07s
   POST https://github.com/hybridgroup/gobot/git-upload-pack
        <- 200 application/x-git-upload-pack-result 9.23m 8.95s

   [3/5]    [showhost][transparent]                                                                    [*:8080]
```

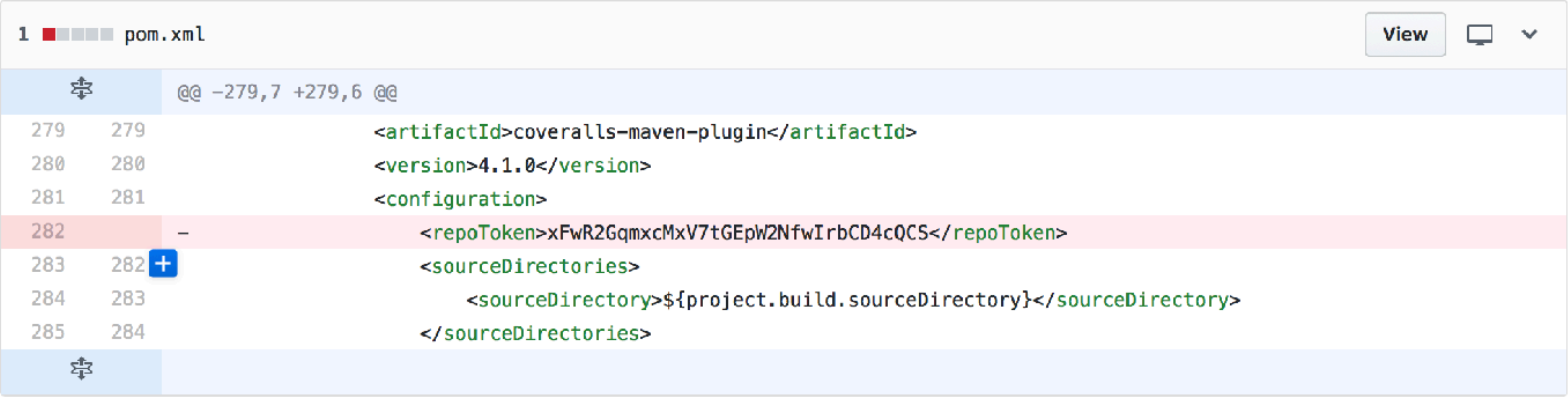
gobot fails:

- No project contact
- No security@ address
- Wrote email to one of the top contributors, reaction within a day: assigned to dev
- dev dropped the ball, since it may be an cloud provider issue
- Lesson to pickup: Do not try to host your own "go" infra unless you have control over everything!
- Still open since April 1st.

Project issues

Apache Incubator: Skywalking (1)

- 17th Mar : There is a repoToken in pom.xml !
- 1,5 h later please file a pull request
- Merged within next hour.



```
@@ -279,7 +279,6 @@
                    <artifactId>coveralls-maven-plugin</artifactId>
                    <version>4.1.0</version>
                    <configuration>
-                       <repoToken>xFwR2GqmxcMxV7tGEpW2NfwIrbCD4cQCS</repoToken>
                        <sourceDirectories>
                            <sourceDirectory>${project.build.sourceDirectory}</sourceDirectory>
                        </sourceDirectories>
```

Skywalking (2)

- Maven is trying to downloading this insecurely (from bro http.log)
- 1521301611.462089 CketVrXC3jqw3xoSi 172.17.0.3 41818 35.186.232.213 80 1 GET repo.spring.io /ext-release-local/org/jboss/shrinkwrap/shrinkwrap-bom/1.2.3/shrinkwrap-bom-1.2.3.pom - 1.1 Apache-Maven/3.5.2 (Java 1.8.0_151; Linux 4.9.60-linuxkit-aufs) 0 80 404 Not Found (empty) - - - - - - F01i8kqElKM97ajU6 - text/json
- Reason <repository> with repo.spring.io in spring-boot.pom

Spring Boot : transitive dependency

Maven dependencies may have its own repositories.
Spring Boot had an insecure repository configuration in its pom

Reported Mar. 24th with pull request
Ack 2 days later
On Mar 27th, a much more in-depth patch was committed in git trunk: Yeah!
Included in 1.5.11 Release on April 5th
Pull request to change spring boot dependency on Jun 11th ack same day.

Apache Camel

- Cleanup of repository was done before
- Bro traces still shows unnecessary, insecure <repositories>
- Pull request on May 2nd, accepted May 7th
- Second on 25th of May, accepted same day.

- Open are calls to google analytics ?!?

```
1523739005.773764       CeLBdP2CjSjsqcchNk      172.17.0.2      46116   216.58.210.14   80      1       GET
www.google-analytics.com        /__utm.gif?utmwv=1&utmn=1755593970&utmcs=UTF-8&utmsr=1440x900&utmsc=32-
bit&utmul=en-us&utmje=1&utmfl=9.0  r28&utmcr=1&utmdt=runtime-2.4.23-jetty/
9.4.6.v20170531&utmhn=7df51ed6aecb&utmr=http://async-io.org&utmp=/runtime/2.4.23/jetty/
9.4.6.v20170531&utmac=UA-31990725-1&utmcc=__utma='-775698071.1076780858.1523739005744.1523739005744.152373900
5744.2;+__utmb=-775698071;+__utmc=-775698071;+__utmz=-775698071.1523739005744.2.2.utmccn=(direct)|
utmcsr=(direct)|utmcmd=(none);+__utmv=-775698071 -      1.1     Java/1.8.0_151 (amd64; Linux 4.9.87-
linuxkit-aufs)      0       35      200     OK      -       -       (empty) -       -       -       -       -
-       FwmNR41yBTzsO16Kvi      -       image/gif
```

-

Apache Servicemix repo

- Misused subversion repo : svn.apache.org/repos/asf/servicemix/m2-repo . Oops.
- Tested again maven central. JAR are ok, pom seem to be handcrafted, MD5 and SHA1 are sometimes only partially valid.
- Three JAR are not legit:
  - jpam-1.1 is compiled with a different compiler
  - jsr-157 is the release bundle from the JSR Process (STAX) and obsoloete
  - jsch-0.1.44 in maven central is corrupt
  - Looks like a repository when back in time it was not clear how to upload things when author doesn't do it. (POM only

Apache plc4x

eclipse hawkbit

- Within a Dockerfile:

```
> gpg --keyserver pgp.mit.edu --recv-keys 385CBC1C7F667FAE
> wget ....
> gpg --batch --verify ...
```

GPG Keyserver is not secure (intended), since there are collision attacks possible on key id. You need to get keys from a trusted party.
Pull request on Feb 18th, accepted Feb 28th.

Oracle j2ee: jaxb

Not part of eclipse jakarta, btw

- Pull request still open since Apr 15th

```
<pluginRepositories>
   <pluginRepository>
     <id>releases.java.net</id>
     <url>http://maven.java.net/content/repositories/releases/</url>
  </pluginRepository>
....
```

Demo of an attack

http://

- Data may be modified in between
- Data are not authenticated
- Data may be from a different server
- Data may be forged by attacker

Attacking

- Men in the middle (MITM) Attack
- Intercepting http traffic
- Demo with ettercap:
  - ARP Poisoning
  - DNS Attack
  - Redirects maven.java.org to own, tainted repository with fake maven-compiler-plugin

Live Hack

- How to attack jaxb implementation ...
- Will start a windows calc.exe when compiling demo

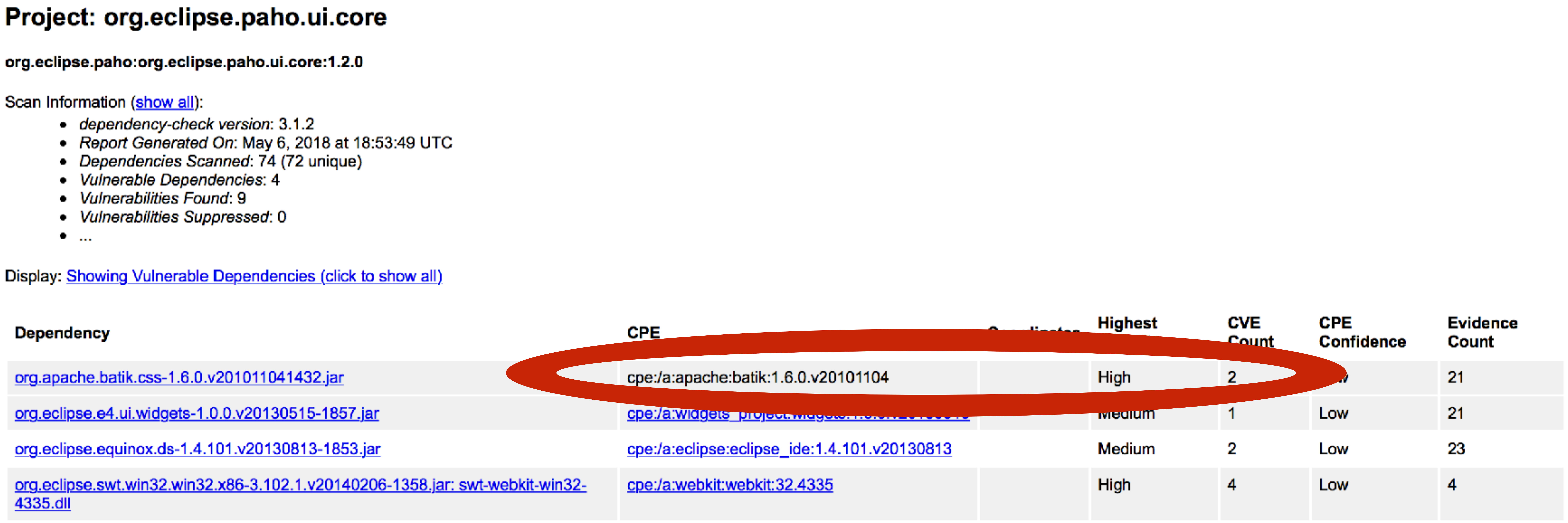
Method 2: Dependency checker

- Insert the OWASP Dependency Checker into pom.xml
  - https://jeremylong.github.io/DependencyCheck/
- Run: mvn verify
- Look at the results (Many false positives)
- Try to patch
- Watch community to iron things out
- Profit

Apache JMeter

Found by OWASP Dependency Checker:
Tripped over outdated Bouncy Castle library.
Submitted a fix in Feb 17th, refined fix committed within 12h !

paho.mqtt.java (eclipse)



Project: org.eclipse.paho.ui.core

org.eclipse.paho:org.eclipse.paho.ui.core:1.2.0

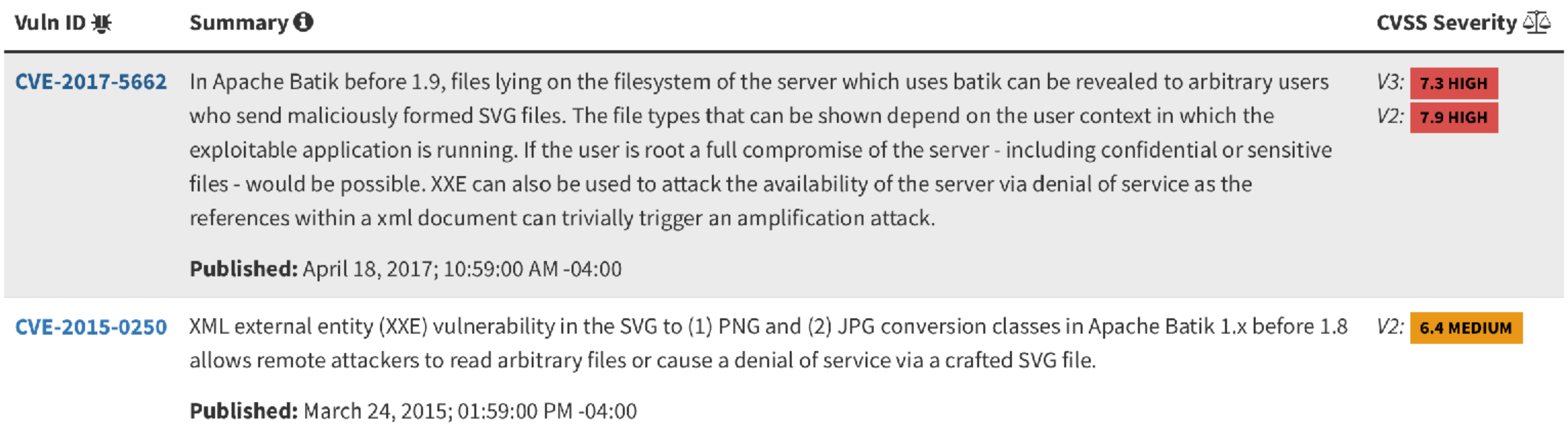
Scan Information (show all):

- *dependency-check version*: 3.1.2
- *Report Generated On*: May 6, 2018 at 18:53:49 UTC
- *Dependencies Scanned*: 74 (72 unique)
- *Vulnerable Dependencies*: 4
- *Vulnerabilities Found*: 9
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	Coordinates	Highest	CVE Count	CPE Confidence	Evidence Count
org.apache.batik.css-1.6.0.v201011041432.jar	cpe:/a:apache:batik:1.6.0.v20101104		High	2	Low	21
org.eclipse.e4.ui.widgets-1.0.0.v20130515-1857.jar	cpe:/a:widgets_project:widgets:1.0.0.v20130515		Medium	1	Low	21
org.eclipse.equinox.ds-1.4.101.v20130813-1853.jar	cpe:/a:eclipse:eclipse_ide:1.4.101.v20130813		Medium	2	Low	23
org.eclipse.swt.win32.win32.x86-3.102.1.v20140206-1358.jar: swt-webkit-win32-4335.dll	cpe:/a:webkit:webkit:32.4335		High	4	Low	4

paho.mqtt.java (eclipse)

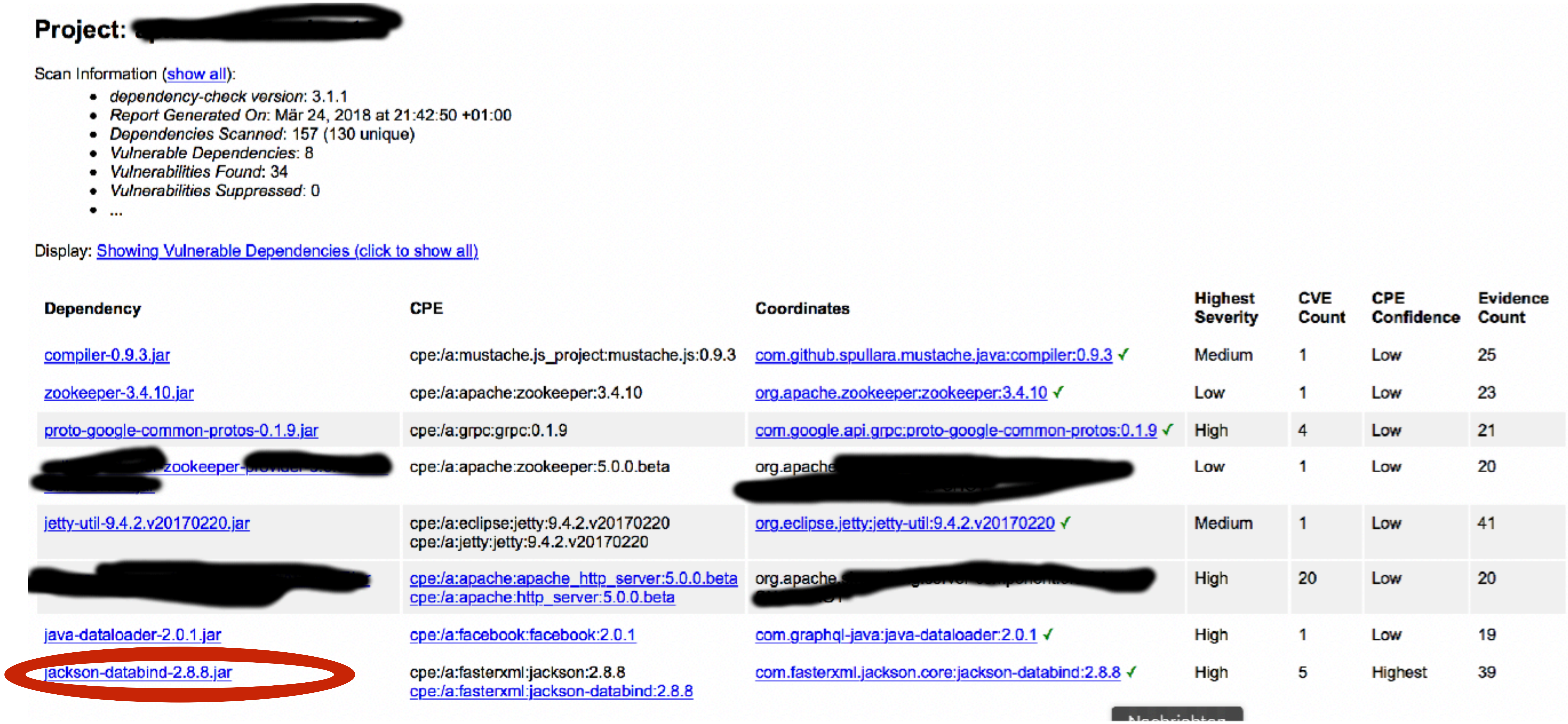


Vuln ID	Summary	CVSS Severity
CVE-2017-5662	In Apache Batik before 1.9, files lying on the filesystem of the server which uses batik can be revealed to arbitrary users who send maliciously formed SVG files. The file types that can be shown depend on the user context in which the exploitable application is running. If the user is root a full compromise of the server - including confidential or sensitive files - would be possible. XXE can also be used to attack the availability of the server via denial of service as the references within a xml document can trivially trigger an amplification attack. **Published:** April 18, 2017; 10:59:00 AM -04:00	*V3:* 7.3 HIGH *V2:* 7.9 HIGH
CVE-2015-0250	XML external entity (XXE) vulnerability in the SVG to (1) PNG and (2) JPG conversion classes in Apache Batik 1.x before 1.8 allows remote attackers to read arbitrary files or cause a denial of service via a crafted SVG file. **Published:** March 24, 2015; 01:59:00 PM -04:00	*V2:* 6.4 MEDIUM

paho.mqtt.java (eclipse)

- Turns out that it uses the release still uses the "kepler" release (2013) unmaintained.
- Trunk uses "mars", same problem.
- Filed pull request to change to "oxygen" via github. Rejected 10days later: Will break thinks but devs want to remove that component anyway, since there are better alternatives.
- RESOLUTION: superseded by mqtt-spy

random project



Project: [redacted]

Scan Information (show all):

- *dependency-check version*: 3.1.1
- *Report Generated On*: Mär 24, 2018 at 21:42:50 +01:00
- *Dependencies Scanned*: 157 (130 unique)
- *Vulnerable Dependencies*: 8
- *Vulnerabilities Found*: 34
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	Coordinates	Highest Severity	CVE Count	CPE Confidence	Evidence Count
compiler-0.9.3.jar	cpe:/a:mustache.js_project:mustache.js:0.9.3	com.github.spullara.mustache.java:compiler:0.9.3 ✓	Medium	1	Low	25
zookeeper-3.4.10.jar	cpe:/a:apache:zookeeper:3.4.10	org.apache.zookeeper:zookeeper:3.4.10 ✓	Low	1	Low	23
proto-google-common-protos-0.1.9.jar	cpe:/a:grpc:grpc:0.1.9	com.google.api.grpc:proto-google-common-protos:0.1.9 ✓	High	4	Low	21
[redacted]	cpe:/a:apache:zookeeper:5.0.0.beta	org.apache[redacted]	Low	1	Low	20
jetty-util-9.4.2.v20170220.jar	cpe:/a:eclipse:jetty:9.4.2.v20170220 cpe:/a:jetty:jetty:9.4.2.v20170220	org.eclipse.jetty:jetty-util:9.4.2.v20170220 ✓	Medium	1	Low	41
[redacted]	cpe:/a:apache:apache_http_server:5.0.0.beta cpe:/a:apache:http_server:5.0.0.beta	org.apache[redacted]	High	20	Low	20
java-dataloader-2.0.1.jar	cpe:/a:facebook:facebook:2.0.1	com.graphql-java:java-dataloader:2.0.1 ✓	High	1	Low	19
jackson-databind-2.8.8.jar	cpe:/a:fasterxml:jackson:2.8.8 cpe:/a:fasterxml:jackson-databind:2.8.8	com.fasterxml.jackson.core:jackson-databind:2.8.8 ✓	High	5	Highest	39

random project

A lot of false positives on OWASP dependency checker.
fasterxml-jackson seems relevant.
A transitive dependency seems to be from jboss resteasy 3.0.7.Final
Was not able to fix it with updating to 3.0.24 since maven dependency resolution kicked in. I did not find the dependency triggering it.
Still open...

Receiving a security report

Fixing
Apache Bigtop

- Apache Bigtop received a security report a few weeks ago
- "Download your stuff securely ... and assign CVE ..."
  - OK, I know about that we do insecure things, but I missed to fixed it in Apache Bigtop, I cared about others.
- Interesting:
- It took me 3 days to discuss how to react, since PMC's are located in asia, usa and europe (me)

Download and Verify

- Download securely from Apache Infra:
- INFRA doesn't like downloads from www.apache.org/dist . Should use mirroring
- But most mirrors are http:// only or not so trusted domains like "klaus-uwe.me"
- See http://maven.apache.org/download.cgi for detailed information how to do it.

Wrap up

Takeaway:
Insecure/Dubious Dependencies

- Maven: Look out for <repository> tags in pom.xml
- Look at transitive dependencies in maven output
- Even well-known frameworks may have serious issues
- In real life you have to do an network analysis

TRUST,
BUT VERIFY IT'S HTTPS://
imgflip.com

Takeaway: Vulnerable Dependencies

- Fix maven dependencies issue is really tough
  - OWASP plugin good, handling complicated
  - Maybe we need support from Apache Maven for logging the dependency resolution for one single artifact
  - You have to be very educated to eliminate the false positives (Example almost every apache .. triggers CVE for Apache http, bzip java implementations triggers CVE reports for C implementation)

FIXING TRANSITIVE
DEPENDENCIES REMAINS HARD
imgflip.com

Takeaway: Infrastructure

- Infrastructure problems:
- If you do not get a response within 5 Days, you likely won't get any response.

5 DAYS
OR NEVER
imgflip.com

Personal wishlist for maven.next

- Bundle essential plugins: Do not download plugins for "clean", or simple java compile
- Make repositories explicit, not implicit in a dependency.
- Write out what triggered the versioning decision.
- Enforce https:// for repositories (like go get)

Questions/Comments?

- Contact me at
  - of ät oflebbe.de
- Slides will be available at www.oflebbe.de