MATERNA
Information & Communications

Apache Tomcat aber sicher!

Frank Pientka, Dortmund

Wer ist Frank Pientka?

Dipl.-Informatiker (TH Karlsruhe)

Software Architect in Dortmund

iSAQB-Gründungsmitglied

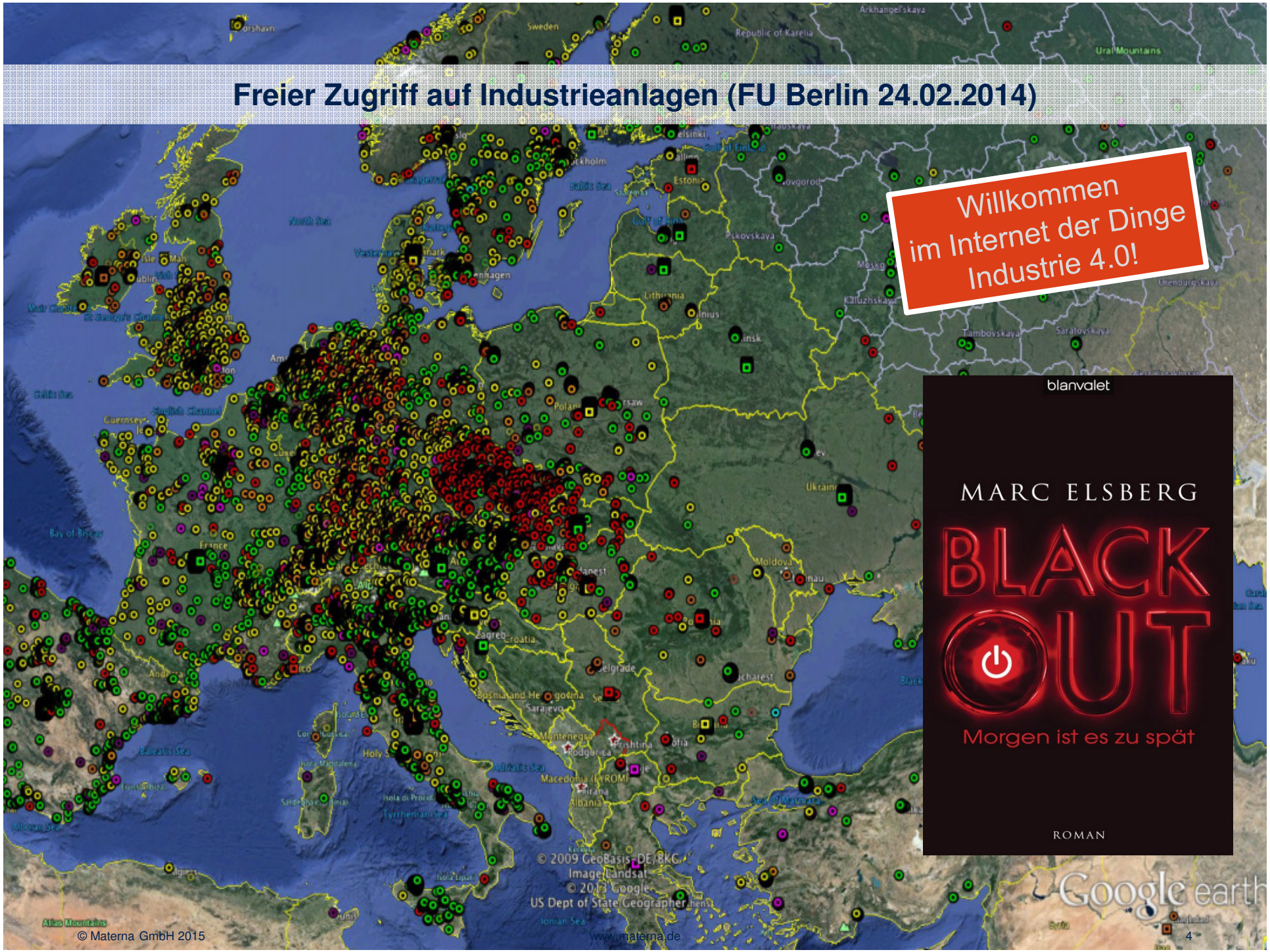
heise.de/developer/Federlesen-Kolumne

Über 20 Jahre IT-Erfahrung
Veröffentlichungen und Vorträge

Wer wir sind.

- Gründung: 1980
  Mitarbeiter: 1.500
  Umsatz 2013: 158 Mio. €
- Inhabergeführtes Familienunternehmen der ITK-Branche
- Full-Service-Dienstleister im Premium-Segment
- Zielgruppe: IT-Organisationen und Fachabteilungen in Privatwirtschaft und Behörden

Freier Zugriff auf Industrieanlagen (FU Berlin 24.02.2014)



SHODAN country:DE city:Darmstadt Coyote port:"8080" Explore Membership Contact Us Blog

Exploits Maps Download Results Create Report

TOP COUNTRIES

Germany	64

TOP CITIES

Darmstadt	64

TOP ORGANIZATIONS

TU Darmstadt, Hochschulrechenzentrum	42
Software AG	5
Hochschule Darmstadt	5
Unitymedia B2B aggregate	3
Deutsche Telekom AG	3

TOP OPERATING SYSTEMS

Windows XP	1
Windows 7 or 8	1
Linux 3.x	1
Linux 2.6.x	1

TOP PRODUCTS

Apache Tomcat/Coyote JSP engine	64

Showing results 1 - 10 of 64

130.83.197.123

jcr-isi-fakdb.ulb.tu-darmstadt.de
TU Darmstadt, Hochschulrechenzentrum
Added on 2015-02-04 16:14:15 GMT
Germany, Darmstadt
Details

```
HTTP/1.0 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://130.83.197.123:8080/de/
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Wed, 04 Feb 2015 16:13:19 GMT
```

Apache Tomcat

130.83.5.128
KH82208.karlshof.wh.tu-darmstadt.de
Linux 3.x
TU Darmstadt, Hochschulrechenzentrum
Added on 2015-02-04 13:49:06 GMT
Germany, Darmstadt
Details

```
HTTP/1.0 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"1887-1418081785000"
Last-Modified: Mon, 08 Dec 2014 23:36:25 GMT
Content-Type: text/html
Content-Length: 1887
Date: Wed, 04 Feb 2015 13:48:00 GMT
```

130.83.197.120

TU Darmstadt, Hochschulrechenzentrum
Added on 2015-02-04 12:34:01 GMT
Germany, Darmstadt
Details

```
HTTP/1.0 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://130.83.197.120:8080/de/
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Wed, 04 Feb 2015 12:30:48 GMT
```

Sicherheitslücke im Herzen des Internets 8.April 2014

07-Apr-2014:	**Security Advisory**: Heartbeat overflow issue.
07-Apr-2014:	OpenSSL 1.0.1g is now **available**, including bug and security fixes
24-Feb-2014:	Beta 1 of OpenSSL 1.0.2 is now **available**, please test it now
06-Jan-2014:	OpenSSL 1.0.0l is now **available**, including bug and security fixes
06-Jan-2014:	OpenSSL 1.0.1f is now **available**, including bug and security fixes

noch mehr Herzbluten …

15-Oct-2014:	OpenSSL 1.0.1j is now **available**, including bug and security fixes
15-Oct-2014:	OpenSSL 1.0.0o is now **available**, including bug and security fixes
15-Oct-2014:	OpenSSL 0.9.8zc is now **available**, including bug and security fixes
25-Sep-2014:	Beta 3 of OpenSSL 1.0.2 is now **available**, please test it now

*56% of devices use versions of OpenSSL more than **50 months** old*
(Cisco 2015 Annual Security Report)

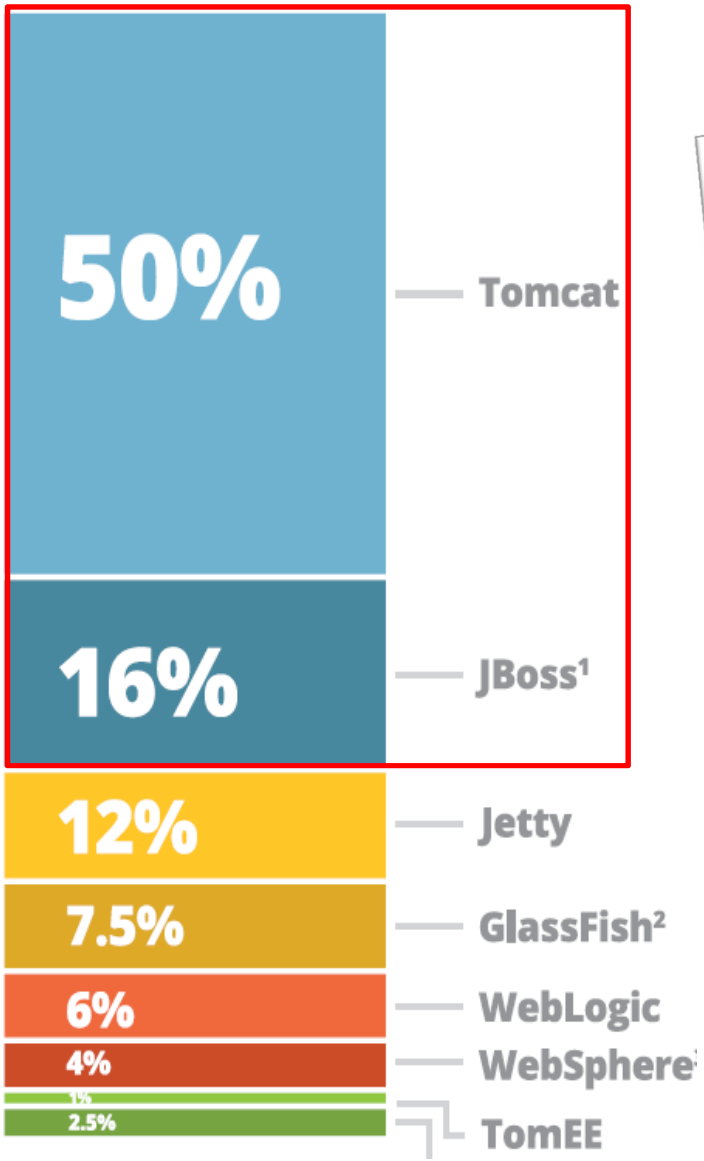
OWASP Top 10 2013

2013-A1 – Injection
2013-A2 – Broken Authentication and Session Management
2013-A3 – Cross Site Scripting (XSS)
2013-A4 – Insecure Direct Object References
2013-A5 – Security Misconfiguration
2013-A6 – Sensitive Data Exposure
2013-A7 – Missing Function Level Access Control
2013-A8 – Cross-Site Request Forgery (CSRF)
2013-A9 – Using Known Vulnerable Components (NEW)
2013-A10 – Unvalidated Redirects and Forwards

Threat Agents	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	Easy	Widespread	Easy	Severe	App / Business Specific
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

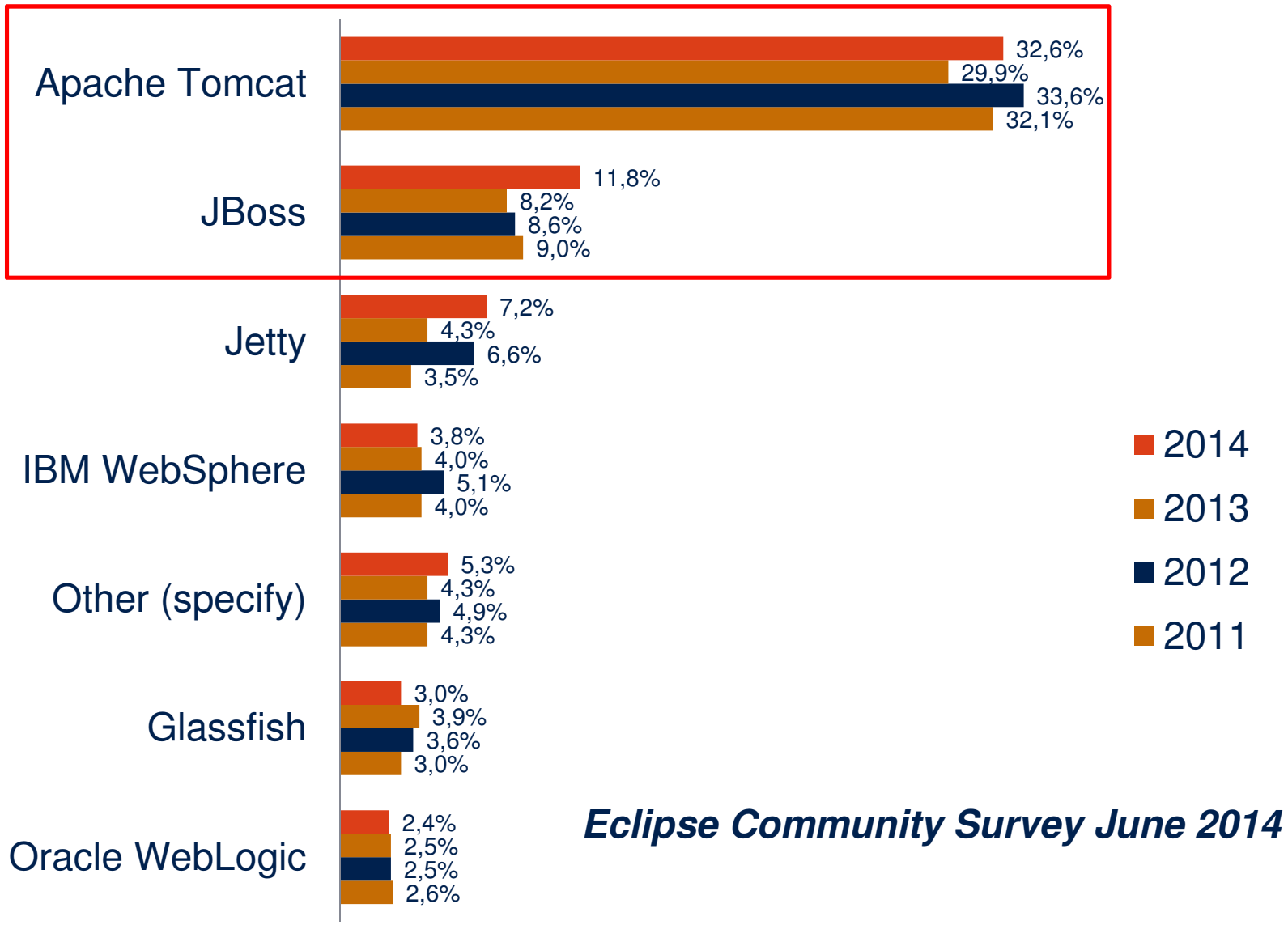
Risk Rating Methodology

Welcher Anwendungsserver wird eingesetzt?



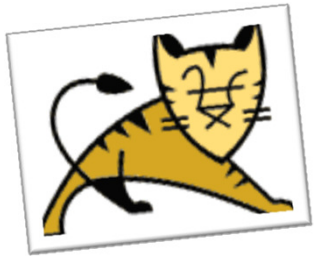
Java tools and technologies report 2014 RebelLabs

Welcher Anwendungsserver wird eingesetzt?



Eclipse Community Survey June 2014

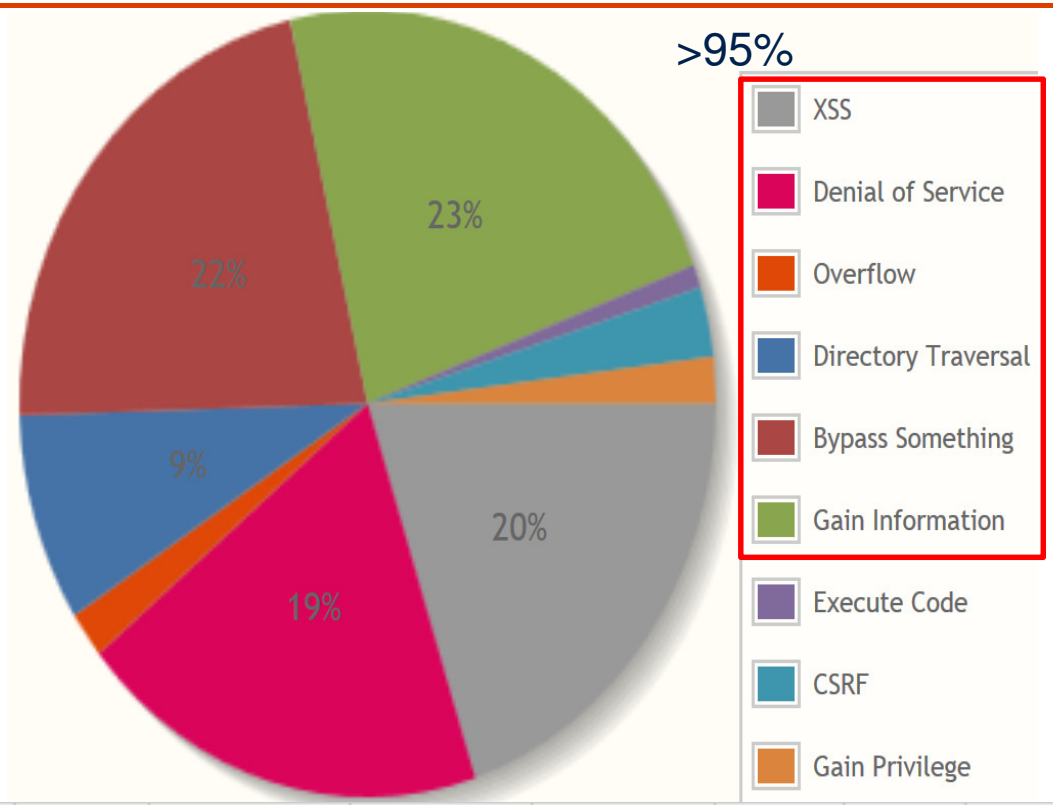
Apache Tomcat Versionen



ab	Servlet	JSP	Tomcat Version	Java, EL, JDBC, TLS Version
2013	**3.1**	**2.3**	**8.0.x (8.0.19)**	**JRE 1.7+(8), EL 3.0, TLS 1.2, JDBC 4.1** (Disabled SSLv3 by default)
2010	3.0	2.2	7.0.x **(7.0.60)**	JRE 1.6+**(8)**, EL 2.2, TLS 1.0, JDBC 4.0
2006	2.5	2.1	6.0.x **(6.0.43)**	JRE 1.5+**(8)**, EL 2.1, TLS 1.0, JDBC 3.0
2004	*2.4*	*2.0*	*5.5.36 (EOL)*	*JDK 1.4+*, EL 1.0, TLS 1.0, JDBC 2.1

http://wiki.apache.org/tomcat/Specifications
http://wiki.apache.org/tomcat/TomcatVersions
Tomcat 9: Servlet 4.0, HTTP/2, JSP 2.4, EL 3.1, WebSocket 1.2

Welche Tomcat-Schwachstellen? (cvedetails.com)

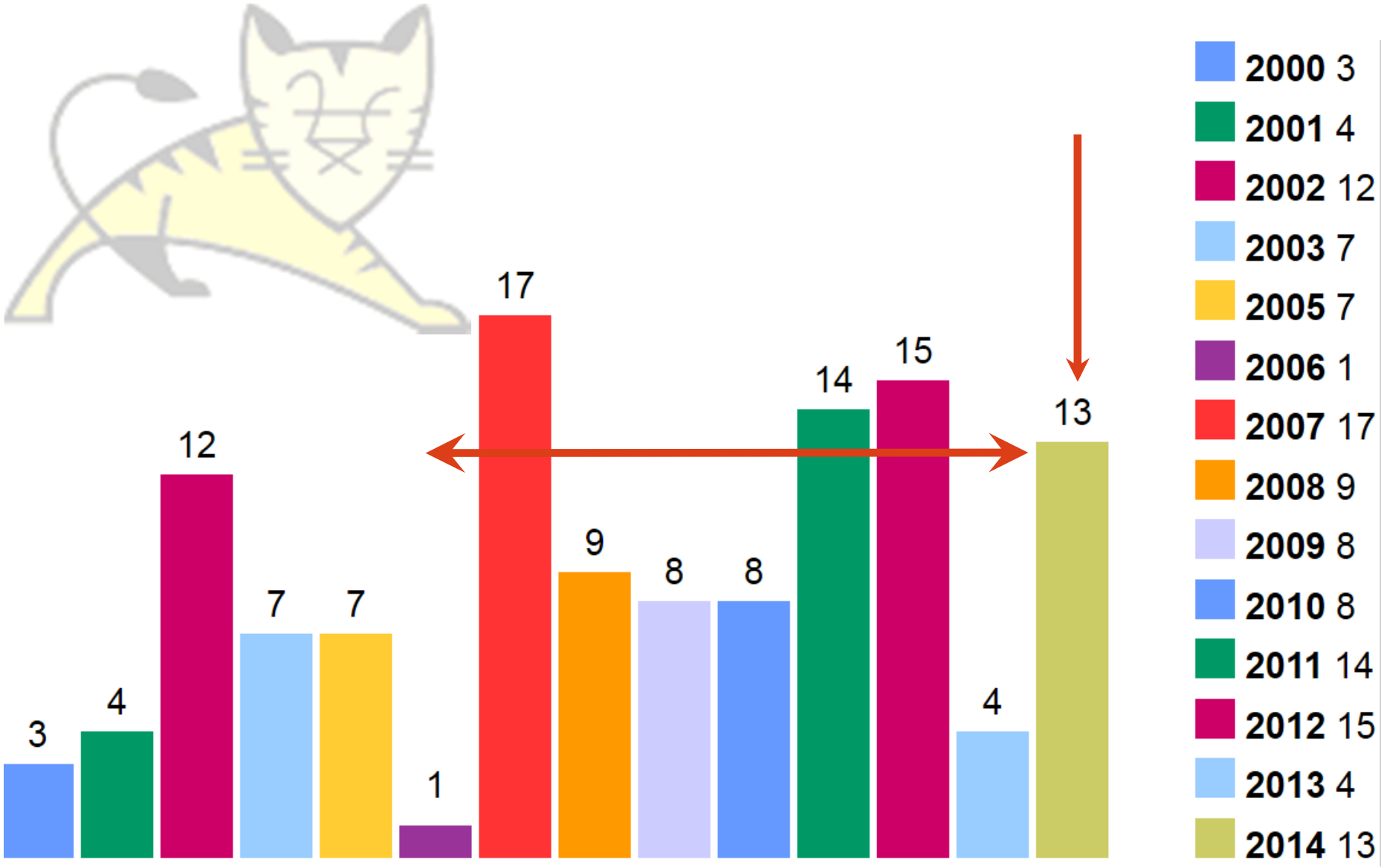


TOP 4 #CVEs
XSS #21
Denial of Service #22
Bypass Something #24
Gain Information #24

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	CVE-2014-0119	264			2014-05-31	2014-09-04	4.3	None	Remote	Medium	Not required

Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provide entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associat web applications on a single Tomcat instance via a crafted web application.

Entwicklung der Tomcat-Schwachstellen? (cvedetails.com)



© Materna GmbH 2015

Tomcat Sicherheit

[ANN] Apache Tomcat 6.0.43 released
[ANN] Apache Tomcat 7.0.57 released
[ANN] Apache Tomcat 8.0.15 available
Re: [ANN] Apache Tomcat Native 1.1.32 released
[ANN] Apache Tomcat Native 1.1.32 released
[ANN] Apache Tomcat 7.0.56 released
[ANN] Apache Tomcat 8.0.14 available
[SECURITY] CVE-2013-4444 Remote Code Execution in Apache Tomcat

7u75 Release Date: 2015-01-19

8u31 Release Date: 2015-01-19

From	bugzi...@apache.org
Subject	Bug report for Tomcat Native [2014/12/07]
Date	Sun, 07 Dec 2014 07:15:49 GMT

```
+-----------------------------------------------------------------------------
| Bugzilla Bug ID
|      +------------------------------------------------------------------------
|      | Status: UNC=Unconfirmed NEW=New         ASS=Assigned
|      |         OPN=Reopened    VER=Verified    (Skipped Closed/Resolved)
|      |    +-------------------------------------------------------------------
|      |    | Severity: BLK=Blocker CRI=Critical  REG=Regression  MAJ=Major
|      |    |           MIN=Minor   NOR=Normal    ENH=Enhancement TRV=Trivial
|      |    |    +--------------------------------------------------------------
|      |    |    | Date Posted
|      |    |    |          +-----------------------------------------------------
|      |    |    |          | Description
|      |    |    |          |
|48655|Inf|Nor|2010-02-02|Active multipart downloads prevent tomcat shutdown
|49038|Inf|Nor|2010-04-02|Crash in tcnative
|52319|Inf|Maj|2011-12-12|Tomcat 6 crashes with [libapr-1.so.0+0x196da]  sig
|52627|New|Min|2012-02-08|Segmentation fault in org.apache.tomcat.jni.File.i
```

Fixed in Apache Tomcat 7.0.54 **released 22 May 2014**

Low: Information Disclosure CVE-2014-0119

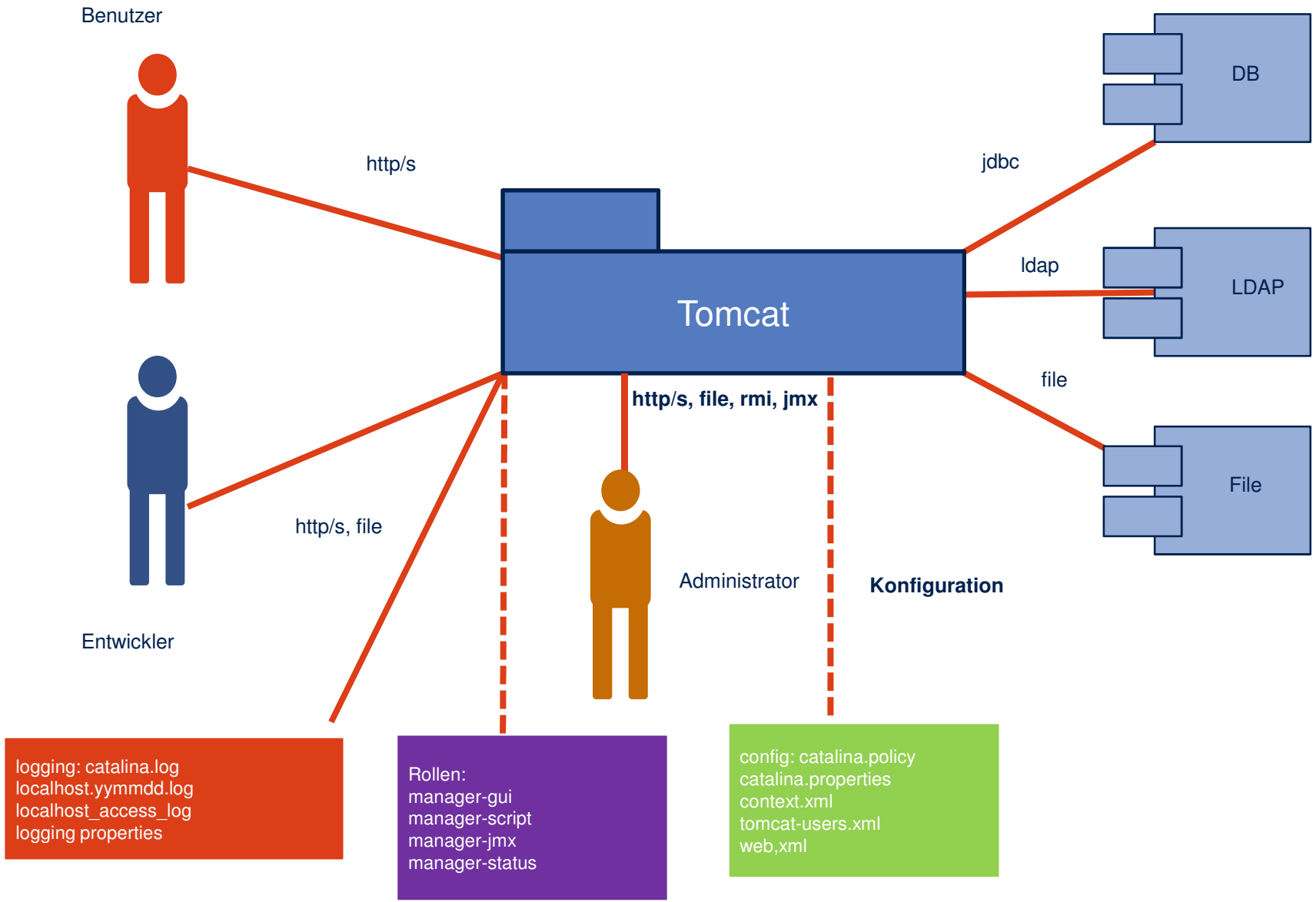
In limited circumstances it was possible for a malicious web application to replace the XML parsers used by Tomcat to process XSLTs for the default servlet, JSP documents, tag library descriptors (TLDs) and tag plugin configuration files. The injected XML parser(s) could then bypass the limits imposed on XML external entities and/or have visibility of the XML files processed for other web applications deployed on the same Tomcat instance.

This was fixed in revisions 1588199, 1589997, 1590028 and 1590036.

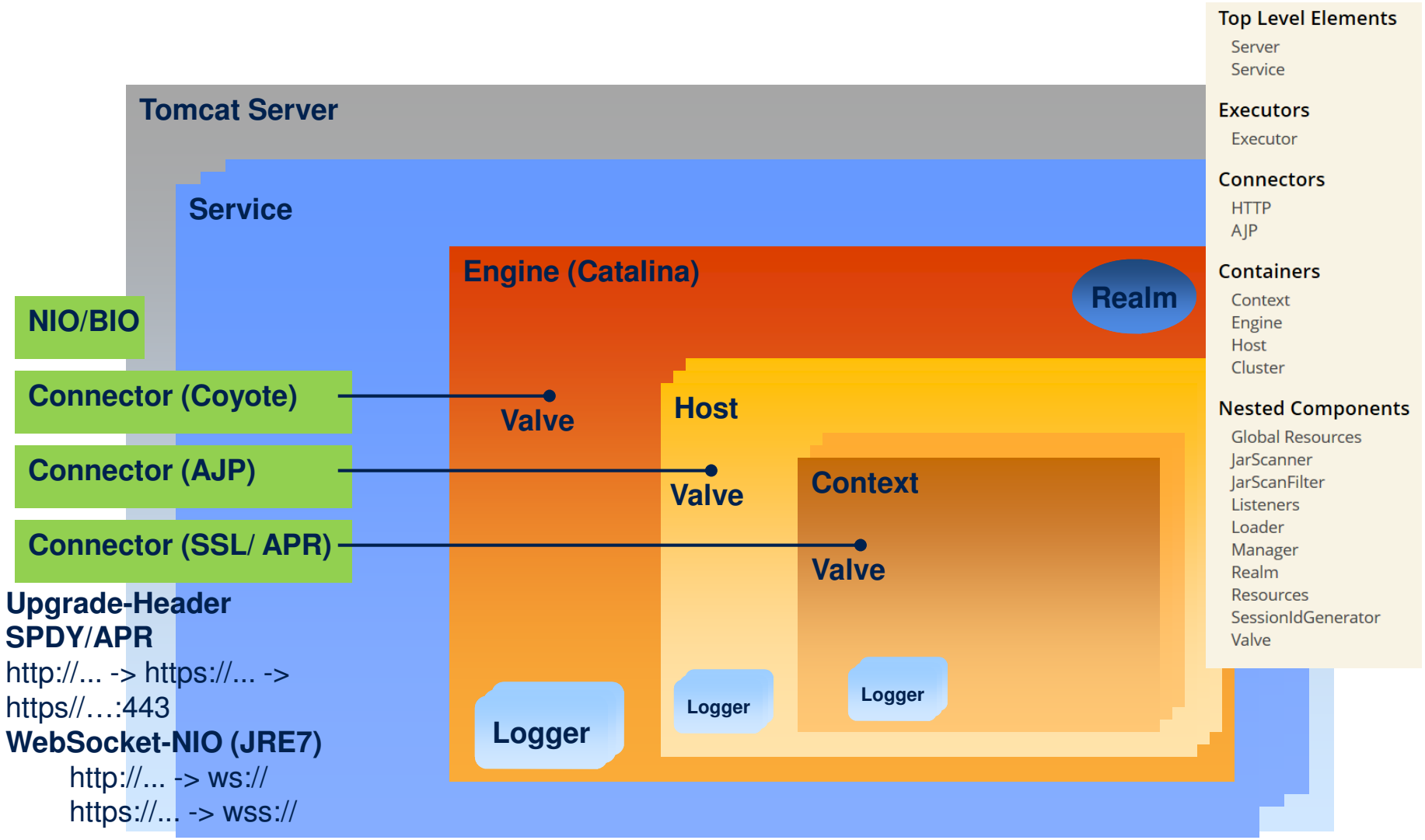
This issue was identified by the Tomcat security team on 12 April 2014 and made public on 27 May 2014.

Affects: 7.0.0-7.0.53

Tomcat-Überblick: Sicherheits-Kontext

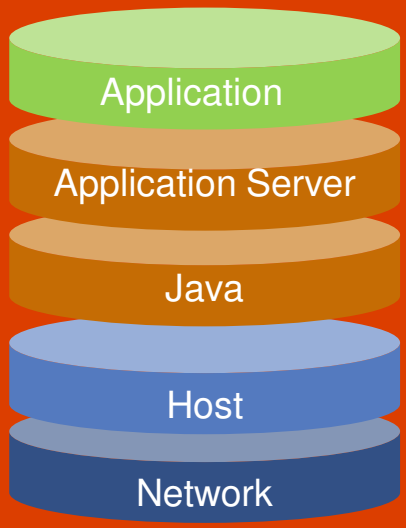


Tomcat Komponenten



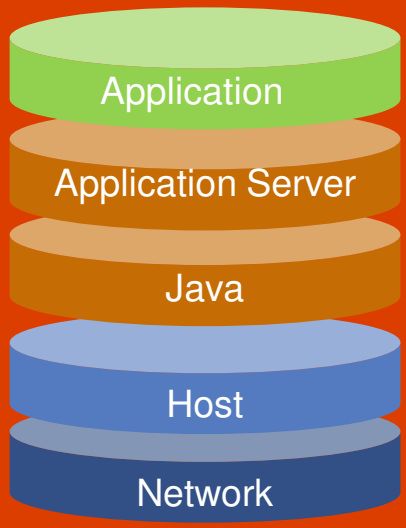
Sicherheit - aber wie?

- Ebenen der Sicherheit
- CVE-/OWASP-Kategorien
- Verschlüsselung, Chiffren, Algorithmen, Zertifikate
- Java, Policy, JCA, lange Schlüssel
- Authentifizierung, Autorisierung, Passwort Hashing
- Konfiguration abspecken, Werte anpassen
- Filtern, Cookies
- ALLE Komponenten aktualisieren



Wie überwachen?

- JMX → Ressourcen-Verbrauch, Grenzwerte
- Logdateien → Auffälligkeiten, Fehlercodes
- Manager Console → Konfiguration, Ressourcen, Anwendungen
- Jar-Versionen → CVEchecker, CVE Dependency-Check
- Chiffrensammlungen → cipherscan
- SSL scanner → SSLyze, SSLScan



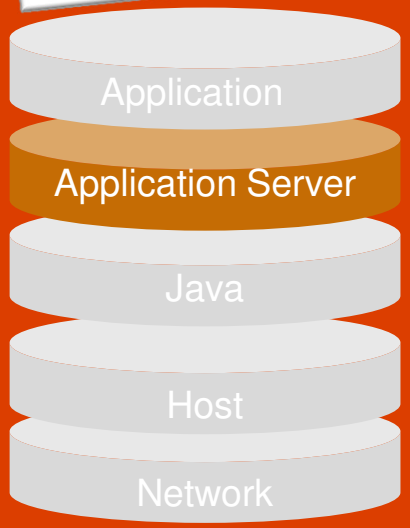
© Materna GmbH 2015

Sicherheit von Anfang an - abspecken

- Installationsdatei verifizieren

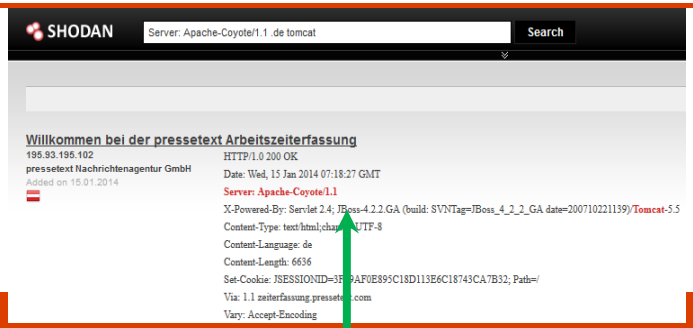
```
md5sum -c apache-tomcat-8.0.17.zip.md5
```

- Aktuelle Versionen (Tomcat, Java, JDBC, HTTP, mod_jk)
- Aufräumen: *webapps, lib, conf* (Hotdeployment, Devmode, Shutdown-Port-Passwort)
- Konfiguration anpassen: `server.xml, web.xml`
- Testen



© Materna GmbH 2015

Tarnen, täuschen - Produktversion verschleiern



CATALINA_HOME/lib

```
jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties
vi ServerInfo.properties server.info=Apache
server.number=0.0.0.0
jar uf catalina.jar
org/apache/catalina/util/ServerInfo.properties
```

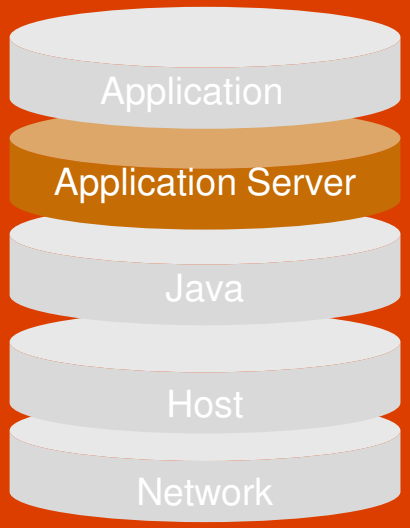
CATALINA_BASE/conf/server.xml

```
<Connector port="8080" ... server="Apache" />
```

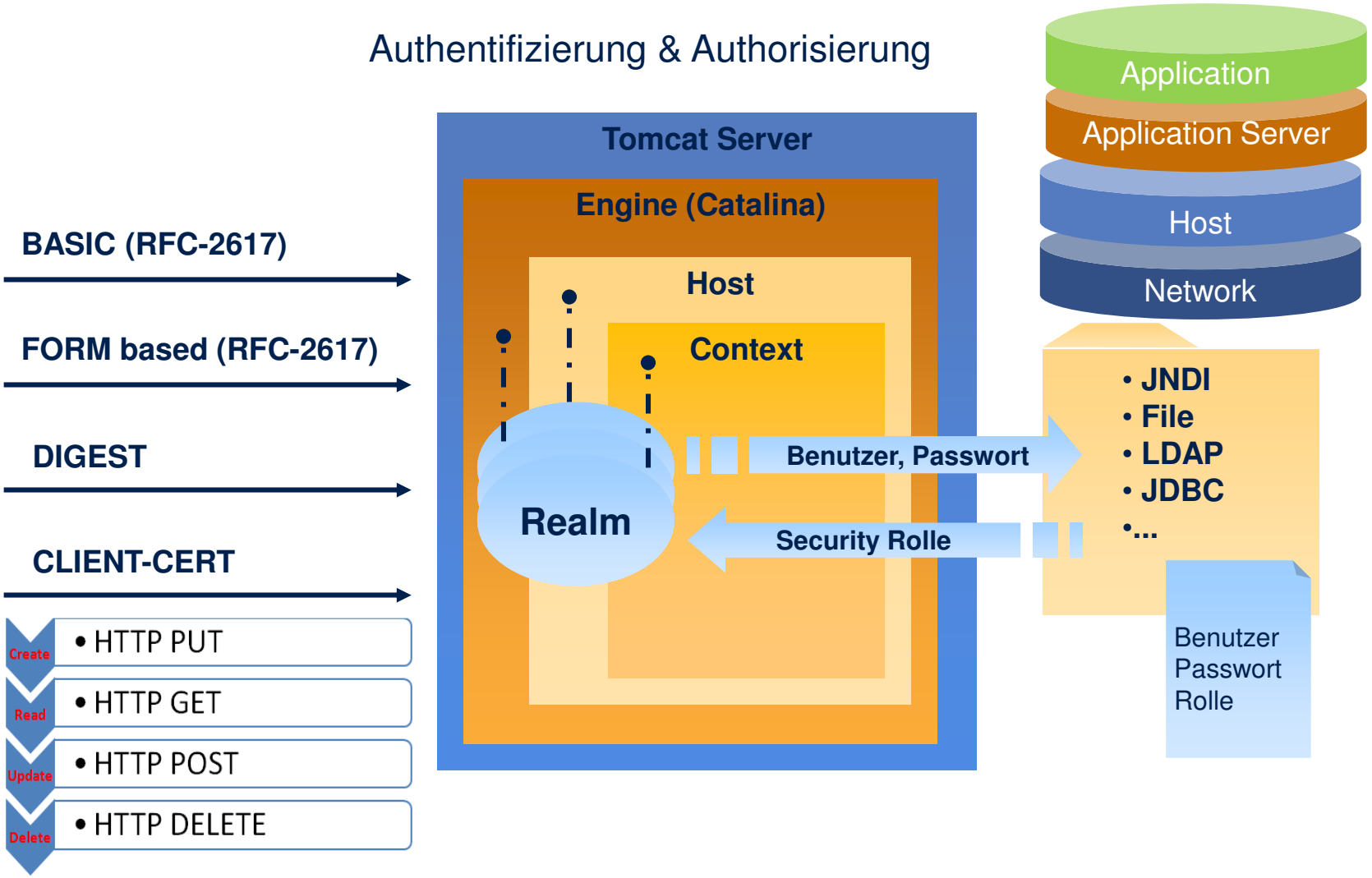
Testen: version.[sh|bat]

```
telnet localhost/index 8080,  wget https://localhost:8443
```

Tomcat 8.0.14, 7.0.57+ `<Listener className="org.apache.catalina.startup.VersionLoggerListener"/>`



Zugriff für Webanwendungen kontrollieren: Wer, Wie, Was?



2013-A2 Broken Authentication: Verschlüsselte Passwörter gestern & heute

OWASP Top 10 für Entwickler-2013

A8 Cross-Site Request Forgery (CSRF, XSRF, Session Riding)

Bedrohungs-quelle	Angriffs-vektor	Schwachstellen		Technische Auswirkung	Auswirkung auf das Unternehemen
———	Ausnutzbarkeit DURCHSCHNITTLICH	Verbreitung HÄUFIG	Auffindbarkeit EINFACH	Auswirkung MITTEL	Application / Business Specific
Jeder, der einem Nutzer einer Webanwendung einen nicht beabsichtigten Request für diese Anwendung unterschieben kann. Hierfür kommt jede Website oder jede HTML-Quelle in Betracht, die der Nutzer verwendet.	Durch Image-Tags, XSS oder andere Techniken löst das Opfer unbeabsichtigt einen gefälschten HTTP-Request für eine Anwendung aus. Falls der Nutzer authentisiert ist, wird dieser Angriff Erfolg haben.	CSRF zielt auf Anwendungen, die es dem Angreifer erlauben, alle Details eines Requests für eine bestimmte Aktion vorherzusagen. Da Browser Informationen zum Session-Management automatisch mitsenden, kann ein Angreifer gefälschte Requests auf bösartigen Websites hinterlegen, die von legitimen Requests nicht unterschieden werden können. CSRF-Schwächen sind leicht durch Penetrationstests oder Quellcode-Analysen auffindbar.		Der Angreifer kann unbemerkt das Opfer über dessen Browser dazu veranlassen, alle Daten zu ändern oder jede Funktion auszuführen, für die das spezifische Opfer berechtigt ist.	Betrachten Sie den Geschäftswert der betroffenen Daten oder Funktionen. Es bleibt die Unsicherheit, ob der Nutzer die Aktion ausführen wollte. Bedenken Sie mögliche Auswirkungen auf Ihre Reputation.

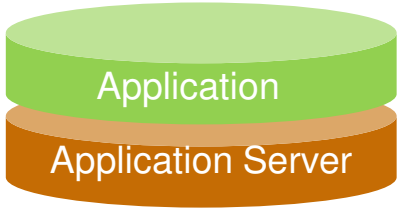
https://www.owasp.org/index.php/Germany/Projekte/Top_10_fuer_Entwickler-2013/A8-Cross-Site_Request_Forgery_%28CSRF%29

Tomcat 6,7,8: org.apache.catalina.filters.CsrfPreventionFilter

XSS-Angriffe: Cookie nicht mehr auslesbar

Seit **Servlet 3.0 WEB-INF/web.xml (default ab Tomcat 7)**

```
<session-config>
    <session-timeout>30</session-timeout>
    <cookie-config>
        <http-only>true</http-only>
    </cookie-config>
    <tracking-mode>COOKIE</tracking-mode>
</session-config>
```



http://jeremylong.github.io/DependencyCheck

Dependency-Check Report

Project: Hello World

Scan Information (show all):

- *dependency-check version*: 1.1.3
- *Report Generated On*: 21.03.2014 13:51:40
- *Dependencies Scanned*: 22
- *Vulnerable Dependencies*: 5
- ...

Dependency Display: show all

- catalina.jar
  - catalina-ant.jar
  - catalina-ha.jar
  - catalina-tribes.jar
- jasper.jar
  - jasper-el.jar
- tomcat-api.jar
  - tomcat-coyote.jar
  - tomcat-dbcp.jar
  - tomcat-i18n-es.jar
  - tomcat-i18n-ja.jar
  - tomcat-util.jar
  - tomcat7-websocket.jar
- tomcat-i18n-fr.jar
- tomcat-jdbc.jar

catalina.jar (cpe:/a:apache:tomcat:7.0.48, cpe:/a:apache_software_foundation:tomcat:7.0.48) : CVE-2013-0346
jasper.jar (cpe:/a:apache:tomcat:7.0.48, cpe:/a:apache_software_foundation:tomcat:7.0.48) : CVE-2013-0346
tomcat-api.jar (cpe:/a:apache:tomcat:7.0.48, cpe:/a:apache_software_foundation:tomcat:7.0.48, cpe:/a:apache_tomcat:apache_tomcat:7.0.48) : CVE-2013-0346
tomcat-i18n-fr.jar (cpe:/a:apache:tomcat:7.0.48, cpe:/a:apache_software_foundation:tomcat:7.0.48, cpe:/a:apache_tomcat:apache_tomcat:7.0.48, cpe:/a:nfr:nfr:7.0.48) : CVE-2013-0346
tomcat-jdbc.jar (cpe:/a:apache:tomcat, cpe:/a:apache_software_foundation:tomcat:1.1.0.1, cpe:/a:apache_tomcat:apache_tomcat:1.1.0.1) : CVE-2013-2185, CVE-2009-2696, CVE-2007-5461, CVE-2002-0493

Dependencies

catalina.jar

File Path: C:\apache-tomcat-7.0.48\lib\catalina.jar
MD5: A94828826CBE650ED16FFCAB553F4BEA
SHA1: FCE4B03BCEEC331E7197C1E8BA1CC2DEFA40E580

Evidence

Related Dependencies

Identifiers

- **cpe:** cpe:/a:apache:tomcat:7.0.48 *Confidence*:HIGH suppress
- **cpe:** cpe:/a:apache_software_foundation:tomcat:7.0.48 *Confidence*:LOW suppress

Published Vulnerabilities

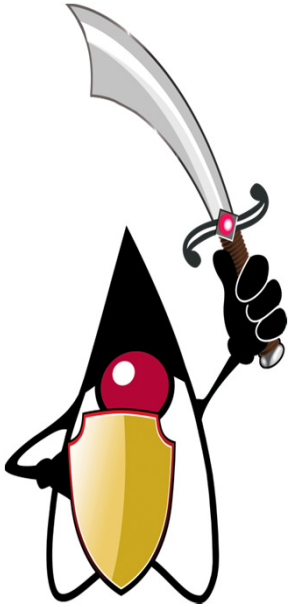
CVE-2013-0346 suppress

A9 - Using Components with Known Vulnerabilities

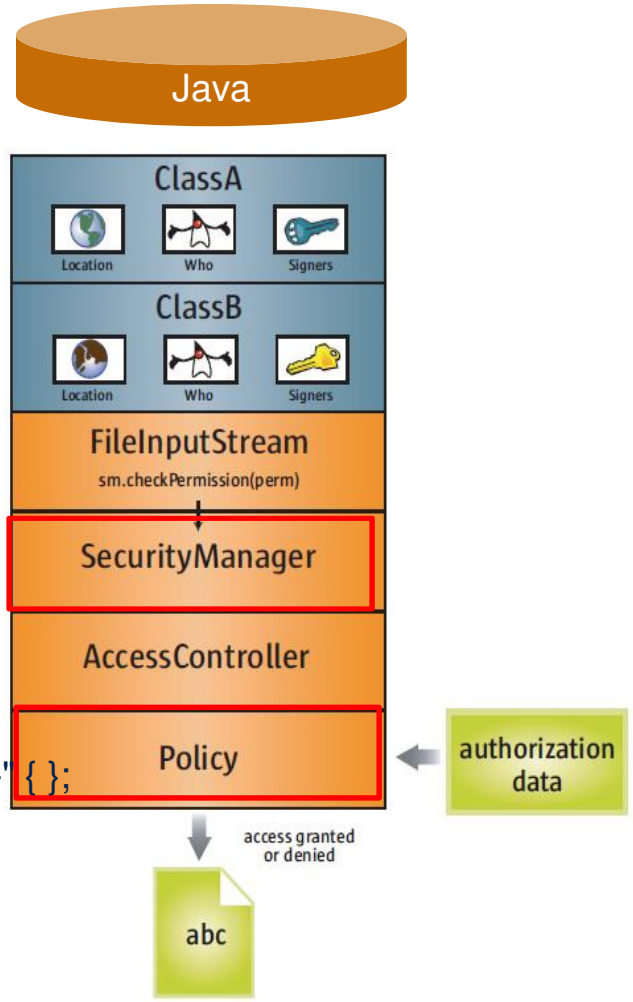
Java-Policies anwenden

conf

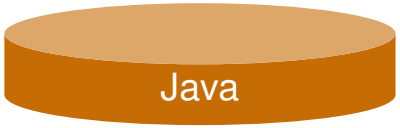
- catalina.properties
- catalina.policy

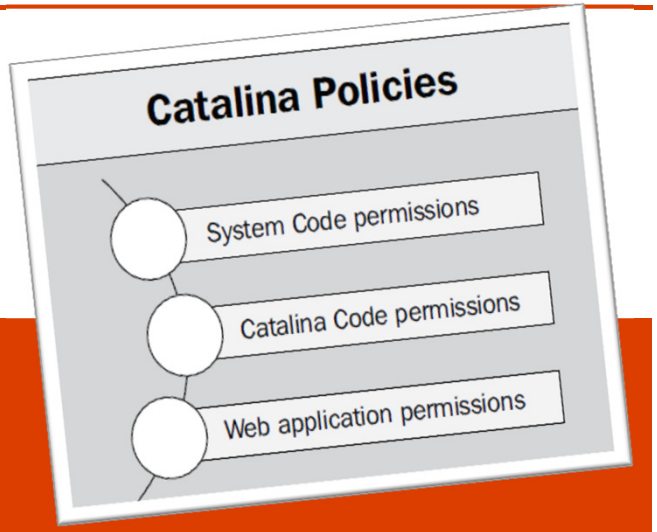


```
// These permissions apply to the servlet API classes
// and those that are shared across all class loaders
// located in the "lib" directory
grant codeBase "file:${catalina.home}/lib/-" {
        permission java.security.AllPermission;
};
// The permissions granted to the context WEB-INF/classes directory
grant codeBase "file:${catalina.base}/webapps/ROOT/WEB-INF/classes/-" { };
```



Sichere Ausführung mit Java-Security-Manager



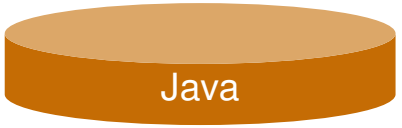


catalina commands:

debug -security	Debug with security manager
run -security	Start in current window with security manager
start -security	Start in separate window with security manager

Beispiel: `catalina run –security`

Längere Schlüssel mit JCE



- **Java Cryptography Extension** (**JCE**)

Unlimited Strength Jurisdiction Policy Files Download

cp local_policy.jar US_export_policy.jar ***jre/lib/security***

- DES = 64 (nachher: 2147483647)
- Triple DES = 128 (nachher: 2147483647)
- **AES** = 128 (nachher: 2147483647=unlimited=256)
- Blowfish = 128 (nachher: 2147483647)
- **RSA** = 2147483647

- **jre\lib\security\java.security:**

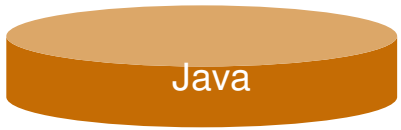
jdk.tls.disabledAlgorithms=MD5, ***SSLv3, DSA, RSA keySize < 2048***

*securerandom.source=file:/dev/urandom (*SHA1PRNG, NativePRNGNonBlocking, Windows-PRNG)

© Materna GmbH 2015

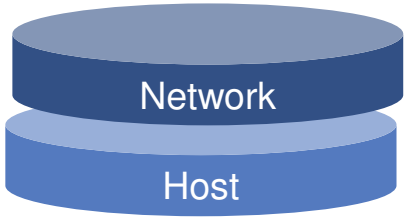
Sicherheitsneuerungen in Java 8

JEP	Title
114	TLS Server Name Indication (**SNI**) Extension
115	**AEAD** CipherSuites
121	Stronger Algorithms for **Password-Based Encryption**
123	Configurable **Secure Random-Number** Generation
124	Enhance the **Certificate Revocation-Checking** API
129	**NSA Suite B** Cryptographic Algorithms
130	**SHA-224** Message Digests
131	**PKCS#11** Crypto Provider for 64-bit Windows
164	**Hardware Acceleration** on Intel and AMD processors
166	Overhaul **JKS-JCEKS-PKCS12 Keystores**



Java9 JEP 229: Create PKCS12 Keystores by Default instead of JKS (since Java1.2)

Welche Chiffren?

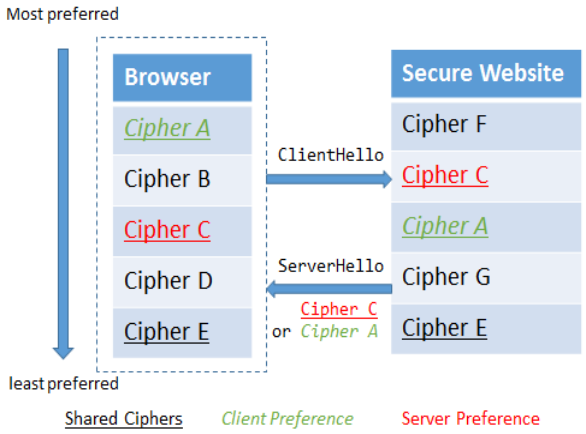


openssl version

openssl ciphers -v

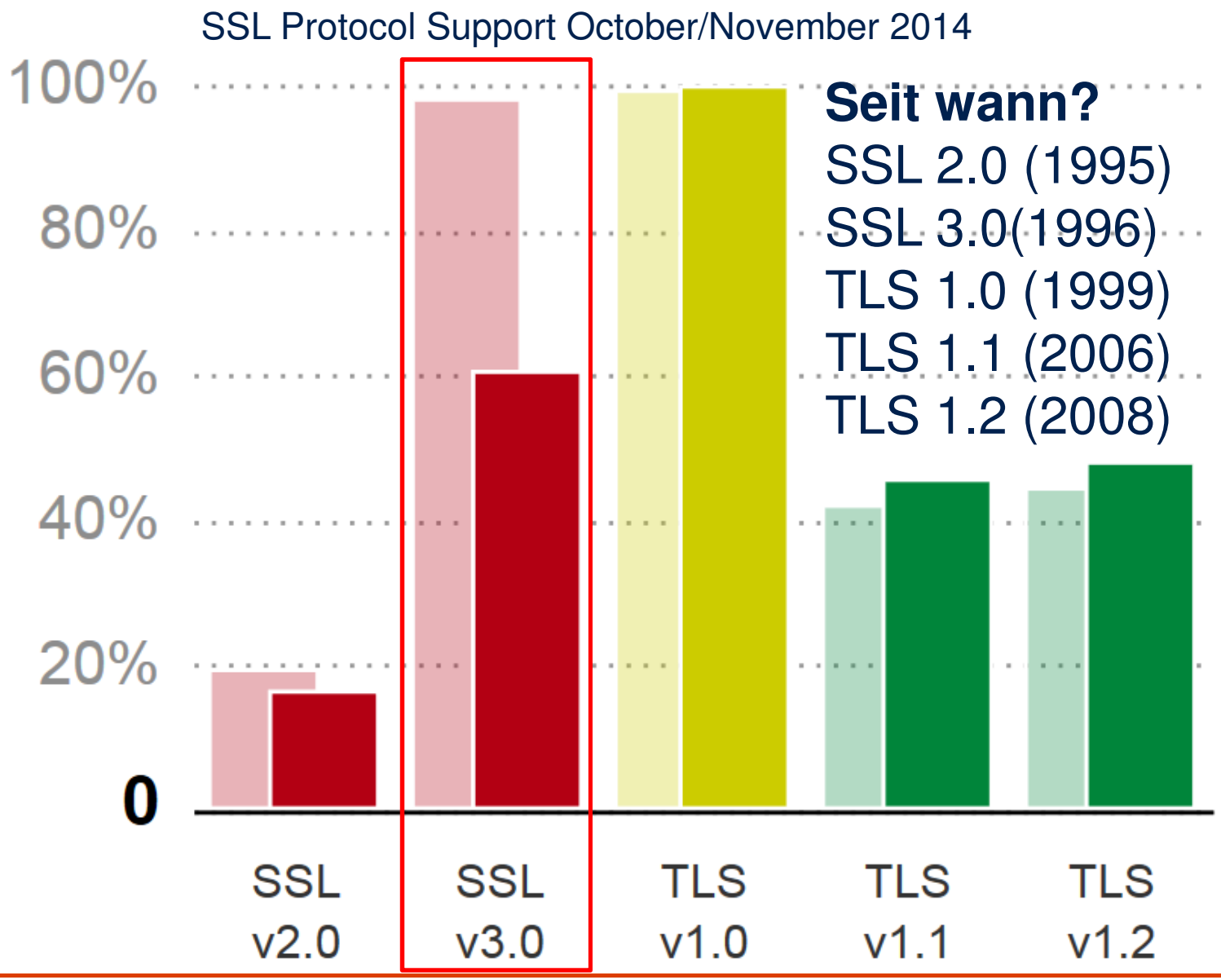
openssl ciphers -V
*‚EECDH+ECDSA+**AESGCMEECDH**+aRSA+ECDSA+SHA256EECDH+aRSA+RC4EDH+aRSAEECDHRC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS‘*

- *TLS_ECDHE_RSA_WITH_RC4_128_SHA*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- ***TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384***
- *TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA*



http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

https://www.trustworthyinternet.org/ssl-pulse



TLS 1.2 erste Wahl – BSI Mindeststandard § 8 Abs. 1 Satz 1 BSIG

heise Security

News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 41 > BSI will TLS 1.2 als Mindeststandard für den Bund

08.10.2013 17:11 « Vorige | Nächste »

BSI will TLS 1.2 als Mindeststandard für den Bund

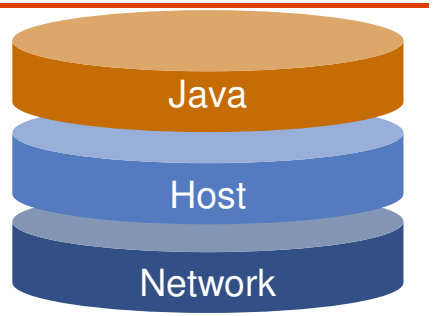
vorlesen / MP3-Download

Ein "Mindeststandard" muss nicht das sein, was der Begriff nahelegt. Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine solche Norm definiert, dann handelt es sich zunächst um eine "unverbindliche Empfehlung". So steht es auch mit dem jetzt verlangten Einsatz von TLS 1.2 als Transportverschlüsselung im Internet. Bundesbehörden sollen ab sofort dieses sichere Verfahren in Verbindung mit Perfect Forward Secrecy (PFS) verwenden. PFS verspricht, auch die nachträgliche Entschlüsselung einer mitgeschnittenen Kommunikation zu verhindern. Verbindlich für die Bundesbehörden wird der jetzige Mindeststandard erst nach Zustimmung des IT-Planungsrats und des Bundesinnenministeriums.

Allerdings, so das BSI, könne eine Migration zu TLS 1.2 "kosten- und zeitintensiv sein". Daher rät es, "bis zur Umstellung zusätzliche Schutzmaßnahmen umzusetzen." Das angreifbare TLS 1.0 dürfe weiterhin eingesetzt werden, wenn Abwehrmaßnahmen gegen bekannte Angriffe wie BEAST ergriffen werden.

Bislang unterstützen Opera, Chrome 30 und der Internet Explorer von Microsoft TLS 1.2. Dort muss der Nutzer es jedoch teilweise erst aktivieren. Die Firefox-Entwickler arbeiten seit längerer Zeit daran, Safari auf Mac OS X nutzt immer noch TLS 1.0. Die iOS-Version des Browsers hingegen nutzt Version 1.2. Auch das dürfte den vom BSI geforderten Umstieg auf TLS 1.2 "auf beiden Seiten der Kommunikationsverbindung" erschweren.

Secure Sockets Layer (SSL) mit Tomcat auf zwei Wegen



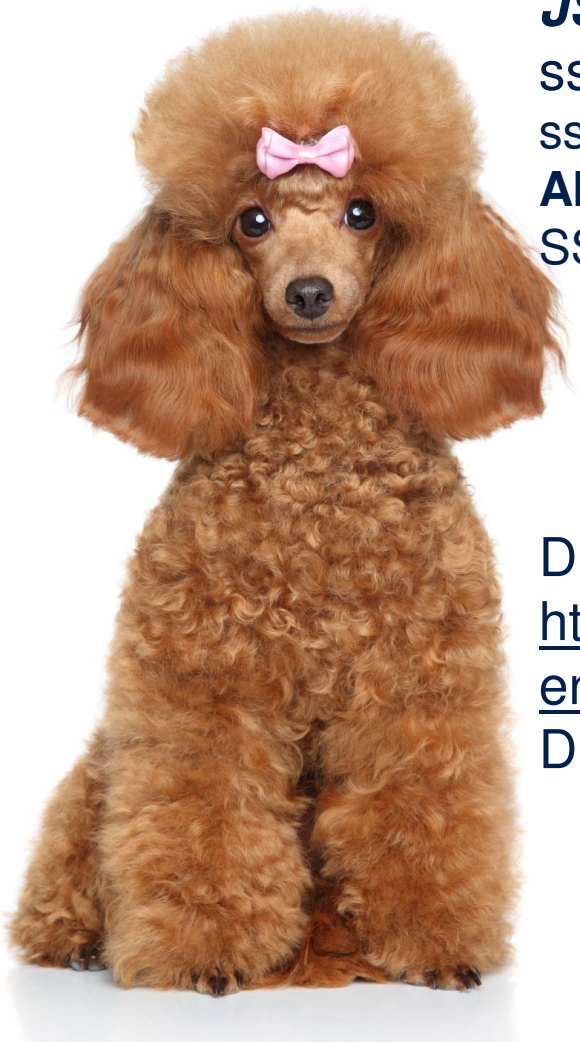
Zwei Konnektoren:

1. **JSSE** protocol="org.apache.coyote.http11.**Http11NioProtocol**“ (**TLS 1.x, d**isable SSLv3 by default >=8.0.15, 7.0.57, 6.0.43)
2. **OpenSSL** 1.0.1j -> **1.1.32, APR 1.5.1** protocol="org.apache.coyote.http11.**Http11AprProtocol**“ (**TLS 1.x**)

Zwei Keystore-Formate:

- **JKS** (Java KeyStore): java **keytool → JEP 229, 166**
- **PKCS12** (Public Key Cryptography Personal Information Exchange Syntax): **OpenSSL**

Bitte keinen Pudel!



server.xml

JSSE:

sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1

APR:

SSLProtocol="TLSv1.2+TLSv1.1+TLSv1"

Browsertest: http://www.poodletest.com
Servertest: http://www.ssllabs.com/ssltest

Disable SSL v3.0 in Oracle JDK and JRE etc.
http://www.oracle.com/technetwork/java/javase/documentation/cve-2014-3566-2342133.html
Disabled in JDK 8u31, 7u76

Schwache Chiffren & SSL 3.0 deaktivieren, lange Schlüssel verwenden

Kontrolle: http://localhost:8080/manager/text/sslConnectorCiphers

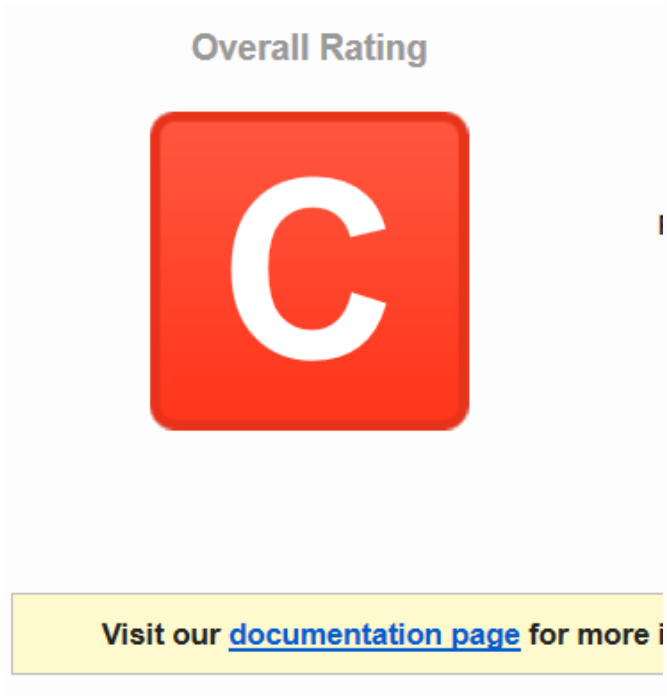
server.xml

<connector port=„8443" maxhttpheadersize="8192" address="127.0.0.1" enablelookups="false" disableuploadtimeout="true" acceptCount="100" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="**TLSv1.2,TLSv1.1,TLSv1**" ciphers="TLS_**ECDHE**_RSA_WITH_**AES_256**_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, SSL_RSA_WITH_**RC4**_128_MD5, SSL_RSA_WITH_**RC4**_128_SHA" keystoreFile="mydomain.key" keystorePass="password" truststoreFile="mytruststore.truststore" truststorePass="password"/>

java -Djavax.net.debug=help *MyApp*

<Connector port="8443" protocol="**org.apache.coyote.http11.Http11AprProtocol**" SSLEnabled="true„ scheme="https" secure="true“ **SSLCertificateFile**="servercert.pem" **SSLCertificateKeyFile**="privkey.pem" SSLPassword="password" clientAuth="false" **SSLHonorCipherOrder**="true“
SSLCipherSuite=„ *EECDH+ECDSA+**AESGCMEECDH**+aRSA+ECDSA+SHA256EECDH+aRSA+RC4EDH+aRSAEECDHRC4*
!aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS“
SSLProtocol="**TLSv1+TLSv1.1+TLSv1.2**" />

SSL Report: xinet.cr-mediateam.de (62.245.238.134)



Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

Cipher Suites (sorted by strength; the server has no preference)

TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_SEED_CBC_SHA (0x96)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

sslyze.exe --regular xinet.cr-mediateam.de

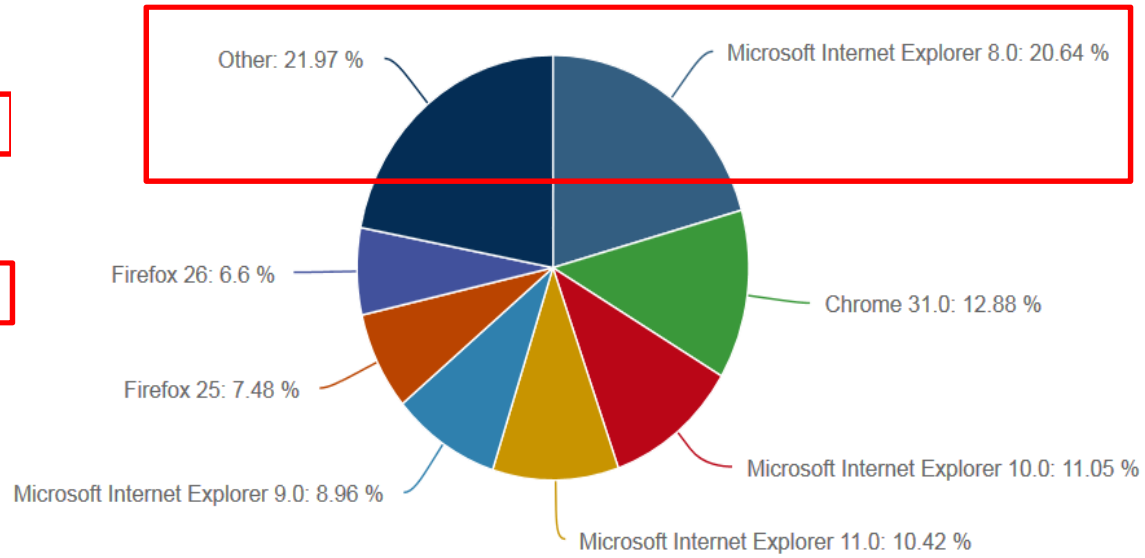
```
SCAN RESULTS FOR XINET.CR-MEDIATEAM.DE:443 -
---------------------------------------------

 * Deflate Compression:
     OK - Compression disabled

 * Session Renegotiation:
     Client-initiated Renegotiations:    VULNE
     Secure Renegotiation:               OK -

 * Certificate - Content:
     SHA1 Fingerprint:                   ddfd3
     Common Name:                        *.cr-
     Issuer:                             Rapid
     Serial Number:                      0FD21
     Not Before:                         Dec 2
     Not After:                          Dec 3
     Signature Algorithm:                sha1W
     Key Size:                           2048
```

```
 * TLSV1_2 Cipher Suites:
     Server rejected all cipher suites.

 * SSLV2 Cipher Suites:
     Server rejected all cipher suites.

Unhandled exception when processing --heartbleed:
socket.error - [Errno 10053] Eine bestehende Verbindung wurde softwareges
durch den Hostcomputer abgebrochen

 * TLSV1_1 Cipher Suites:
     Server rejected all cipher suites.

 * TLSV1 Cipher Suites:
     Preferred:
                  AES256-SHA                -          256 bits

     Accepted:
                  AES256-SHA                -          256 bits
                  SEED-SHA                  -          128 bits
                  RC4-SHA                   -          128 bits
                  RC4-MD5                   -          128 bits
                  AES128-SHA                -          128 bits
                  DES-CBC3-SHA              -          112 bits
                  DES-CBC-SHA               -          56 bits


 * SSLV3 Cipher Suites:
     Accepted:
                  AES256-SHA                -          256 bits
                  SEED-SHA                  -          128 bits
```

Apache https / Tomcat mit OpenSSL 1.0 Chiffrensammlung+Schlüssellänge

Cipher suite name	Protocol	KeyX	Auth	Enc	bit	Hash	Comp.
ECDHE-RSA-AES256-SHA*	TLS 1.0	ECDHE	ECDSA	AES	256	SHA	
ECDHE-RSA-AES128-SHA*	TLS 1.0	ECDHE	ECDSA	AES	128	SHA	
DHE-RSA-AES256-SHA	TLS 1.0	DHE	RSA	AES	256	SHA	
DHE-RSA-AES128-SHA	TLS 1.0	DHE	RSA	AES	128	SHA	
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4	128	SHA	
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES	168	SHA	

- Firefox & Chrome
- Opera
- Windows XP/2000/2003 (IE7/IE8)
- Windows 7/2008R2 (IE8)
- Windows Vista/2008R1 (IE8/7)
- Safari (MacOSx)



http://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers

Browser	Version	SSL 3.0 (insecure)	TLS 1.0	TLS 1.1	TLS 1.2
Chrome	26–29	Enabled by default	Yes	Yes	No
	30–32	Enabled by default	Yes	Yes	Yes
	33–38	Enabled by default	Yes	Yes	Yes
	39				
	40	Disabled by default	Yes	Yes	Yes
Firefox	23	Enabled by default	Yes	Disabled by default	No
	24–26 ESR 24	Enabled by default	Yes	Disabled by default	Disabled by default
	27–33.1 ESR 31.0–31.2	Enabled by default	Yes	Yes	Yes
	ESR 31.3	Disabled by default	Yes	Yes	Yes
	34				
	35				
	36	Disabled by default	Yes	Yes	Yes
Internet Explorer	6	Enabled by default	Disabled by default	No	No
	7, 8	Enabled by default	Yes[	No	No
	7, 8, 9	Enabled by default	Yes	No	No
	8, 9, 10	Enabled by default	Yes	Disabled by default	Disabled by default[
	10				
	11	Enabled by default	Yes	Yes	Yes

Windows 7,8

https://www.ssllabs.com/ssltest/viewMyClient.html

You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser (Experimental)

User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0

QUALYS SSL LABS

Details

Protocols*

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No

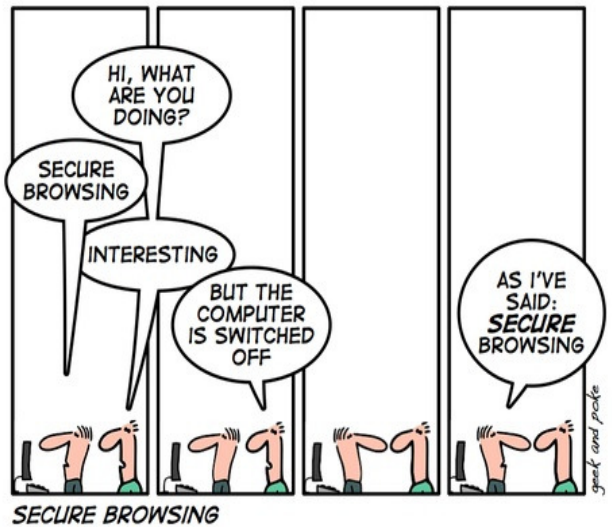
(*) This test reliably detects only the highest supported protocol.

Cipher Suites (in order of preference)

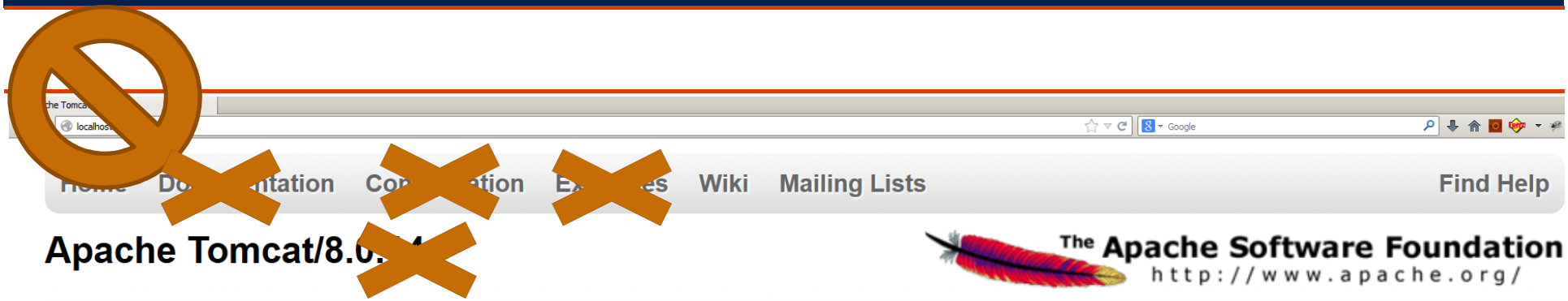
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0xff)	-
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Forward Secrecy	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) Forward Secrecy	256
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x87) Forward Secrecy*	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) Forward Secrecy	256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x38) Forward Secrecy*	256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)	256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Forward Secrecy	128

Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	No
Signature algorithms	-
Elliptic curves	secp256r1, secp384r1, secp521r1
Next Protocol Negotiation	Yes
Application Layer Protocol Negotiation	No
Handshake format	SSL 3+



SECURE BROWSING



Wiki Mailing Lists Find Help

Apache Tomcat/8.0.

The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup | Realms & AAA | Examples | Servlet Specifications

Fazit: Apache Tomcat aber sicher!

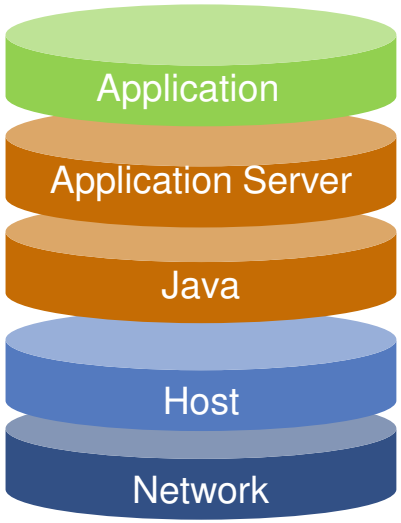
- Ist SSL wirklich sicher?
- Tomcat ist bedroht!
- Wie groß ist die Bedrohung?
- Sicherheit von Anfang an: default is faul(t)
- Mehrstufige Verteidigungsstrategie!
- Der Weg ist das Ziel

Sind Sie sicher?

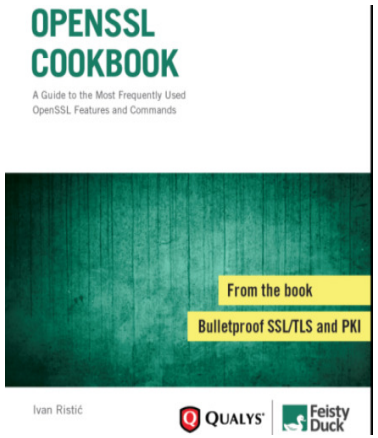
Muss ich das jetzt auch noch tun …

Ausblick – Kryptokalypse?

- TLS 1.2 **ist sicher** SSL 3 **nicht**, wenn **korrekt eingestellt!**
- **Clients** hinken bei Sicherheit **Server** hinterher
- **Sicherheit kostet!**
- **Kenne deine** Systeme, Angreifer und Waffen!



Weitere Infos



Ein freier Kater ohne Sicherheitslücken

Apache Tomcat 8 – aber sicher

Frank Pientka

Apache Tomcat zählt zu den am meisten verwendeten Webservern im Java-Bereich. Da er für unternehmenskritische Anwendungen eingesetzt wird, ist er ein potenzielles und beliebtes Angriffsziel. Der Artikel diskutiert mögliche Angriffsszenarien und deren Lösungen mit Tomcat 8.

Ist Open Source sicherer oder nur anders?

Bundesamt für Sicherheit in der Informationstechnik

Sicherheitsuntersuchung des Apache Jakarta Tomcat Servlet Containers

Feinkonzept

the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Apache Tomcat 5.5/6.0

Version 1.0.0
December 12th, 2009

Weitere Infos

Java Dokumentation

https://bugs.openjdk.java.net/browse/JDK

http://docs.oracle.com/javase/8/docs/technotes/guides/security

Tomcat 8 Dokumentation

http://tomcat.apache.org/security.html

http://tomcat.apache.org/tomcat-80-doc/security-howto.html,
http://wiki.apache.org/tomcatq/FAQ/Security

http://www.mulesoft.com/improving-apache-tomcat-security-step-step-guide

OWASP-Empfehlungen für Tomcat

https://www.owasp.org/index.php/Securing_tomcat

https://wiki.mozilla.org/Security/Server_Side_TLS

SSL/TLS Deployment Best Practices, Ivan Ristić, v1.3, 2013

https://www.ssllabs.com/ssltest

SSLyze SSL Scanner

https://github.com/iSECPartners/sslyze

BSI Sicherheitsuntersuchung des Apache Jakarta Tomcat, 2006

CIS Apache Tomcat 5.5/6.x Server Security Benchmark v1.0.0, 2009

Tomcat aber sicher, Frank Pientka, **JavaSpektrum 04/2014**

Schneller Kater, Frank Pientka, **JavaSpektrum 06/2014**

Vielen Dank für Eure Aufmerksamkeit!

MATERNA GmbH
Dipl. Inform. Frank Pientka
Software Architect
Business Line Digital Enterprise
Telefon: +49 231 5599-8854
Telefax: +49 231 5599-272
E-Mail: Frank.Pientka@materna.de
http://xing.to/frank_pientka