1. – 4. September 2014
in Nürnberg

Herbstcampus

Wissenstransfer
par excellence

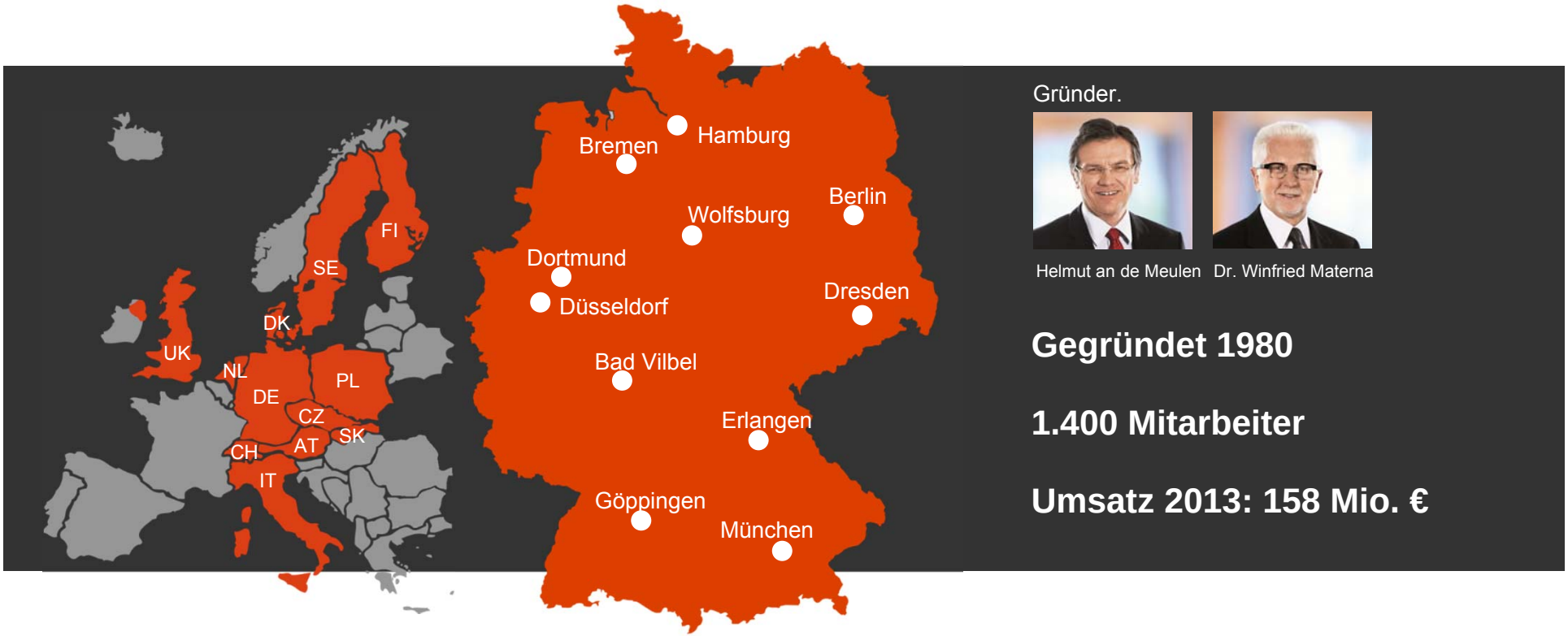
Kryptokalypse now?

Tomcat – aber sicher!

Frank Pientka

Materna GmbH

Wer ist Materna?



Gründer.

Helmut an de Meulen

Dr. Winfried Materna

Gegründet 1980

1.400 Mitarbeiter

Umsatz 2013: 158 Mio. €

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 zu:

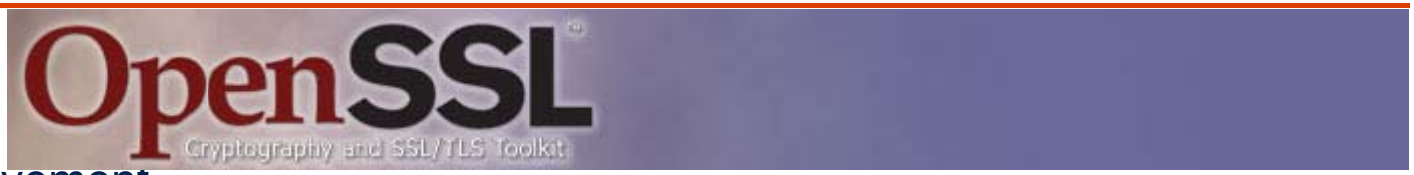
Datenbanken, Applikations- und Portalserver

Sicherheitslücke im Herzen des Internets 8.April 2014

06-Aug-2014:	**Security Advisory**: nine security fixes
06-Aug-2014:	OpenSSL 1.0.1i is now **available**, including bug and security fixes
06-Aug-2014:	OpenSSL 1.0.0n is now **available**, including bug and security fixes
06-Aug-2014:	OpenSSL 0.9.8zb is now **available**, including bug and security fixes
22-Jul-2014:	Beta 2 of OpenSSL 1.0.2 is now **available**, please test it now
30-Jun-2014:	**Project roadmap** released
24-Jun-2014:	**Team status changes** including six new development team members
05-Jun-2014:	**Security Advisory**: seven security fixes
05-Jun-2014:	OpenSSL 1.0.1h is now **available**, including bug and security fixes
05-Jun-2014:	OpenSSL 1.0.0m is now **available**, including bug and security fixes
05-Jun-2014:	OpenSSL 0.9.8za is now **available**, including bug and security fixes
23-Apr-2014:	**Team status changes** including new team member: Steve Marquess
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 …

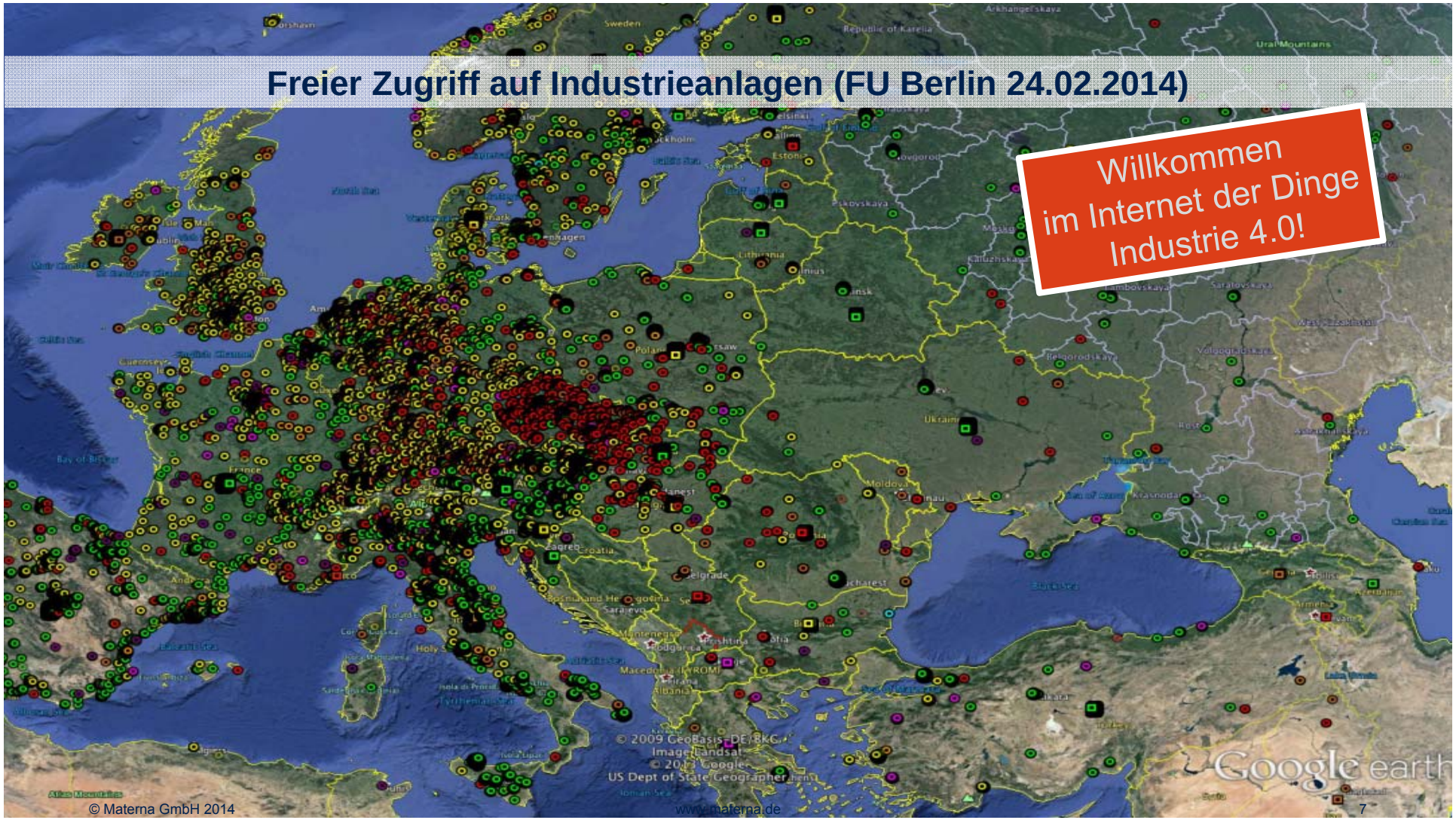
https://www.openssl.org/about/roadmap.html

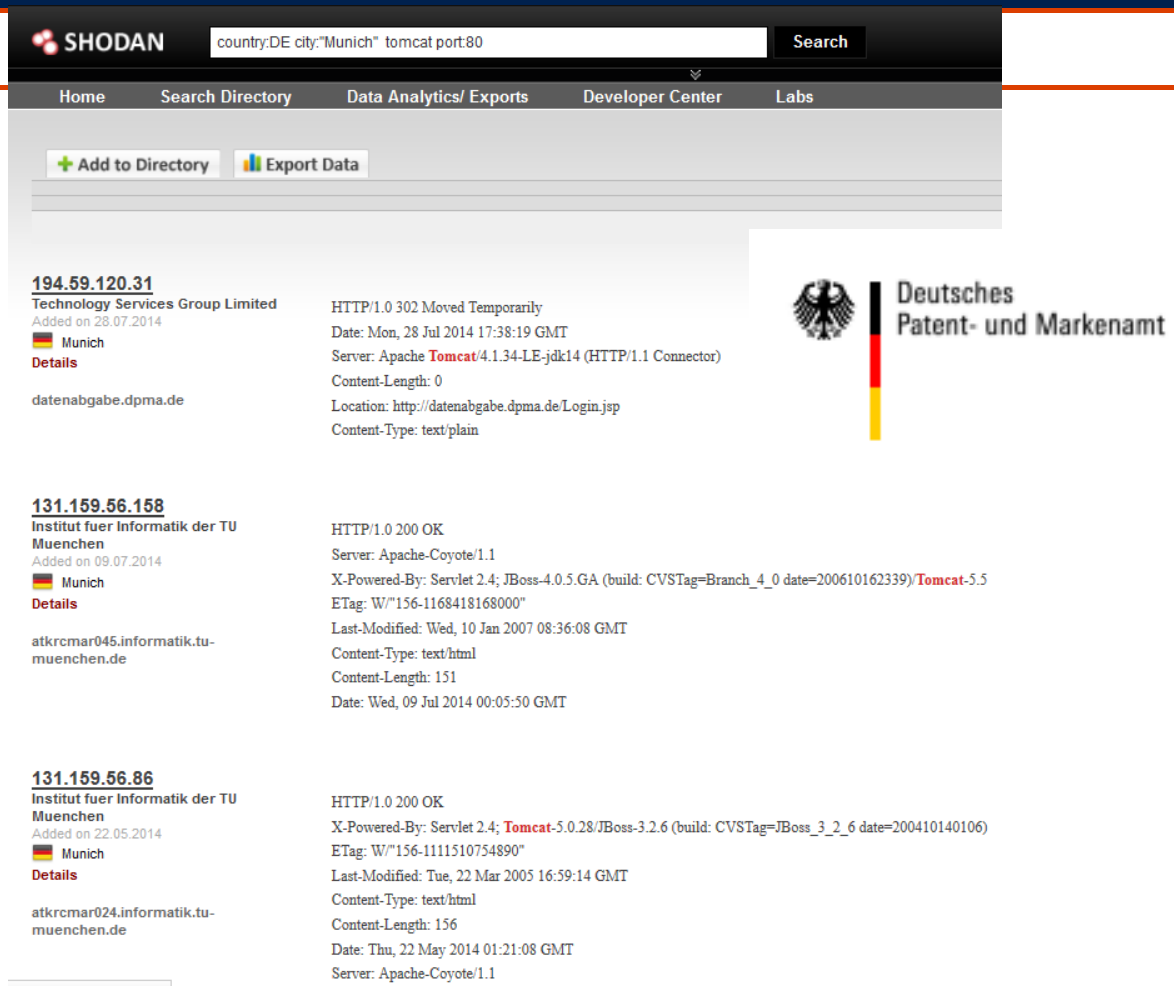


objectives for improvement

- RT Backlog
- Incomplete/incorrect documentation
- Library complexity
- Inconsistent coding style
- Lack of code review
- No clear release plan
- No clear platform strategy

Freier Zugriff auf Industrieanlagen (FU Berlin 24.02.2014)




SHODAN
country:DE city:"Munich" tomcat port:80
Search
Home
Search Directory
Data Analytics/ Exports
Developer Center
Labs
Add to Directory
Export Data
194.59.120.31
Technology Services Group Limited
Added on 28.07.2014
Munich
Details
datenabgabe.dpma.de
HTTP/1.0 302 Moved Temporarily
Date: Mon, 28 Jul 2014 17:38:19 GMT
Server: Apache Tomcat/4.1.34-LE-jdk14 (HTTP/1.1 Connector)
Content-Length: 0
Location: http://datenabgabe.dpma.de/Login.jsp
Content-Type: text/plain
Deutsches
Patent- und Markenamt
131.159.56.158
Institut fuer Informatik der TU Muenchen
Added on 09.07.2014
Munich
Details
atkrcmar045.informatik.tu-muenchen.de
HTTP/1.0 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.5.GA (build: CVSTag=Branch_4_0 date=200610162339)/Tomcat-5.5
ETag: W/"156-1168418168000"
Last-Modified: Wed, 10 Jan 2007 08:36:08 GMT
Content-Type: text/html
Content-Length: 151
Date: Wed, 09 Jul 2014 00:05:50 GMT
131.159.56.86
Institut fuer Informatik der TU Muenchen
Added on 22.05.2014
Munich
Details
atkrcmar024.informatik.tu-muenchen.de
HTTP/1.0 200 OK
X-Powered-By: Servlet 2.4; Tomcat-5.0.28/JBoss-3.2.6 (build: CVSTag=JBoss_3_2_6 date=200410140106)
ETag: W/"156-1111510754890"
Last-Modified: Tue, 22 Mar 2005 16:59:14 GMT
Content-Type: text/html
Content-Length: 156
Date: Thu, 22 May 2014 01:21:08 GMT
Server: Apache-Coyote/1.1

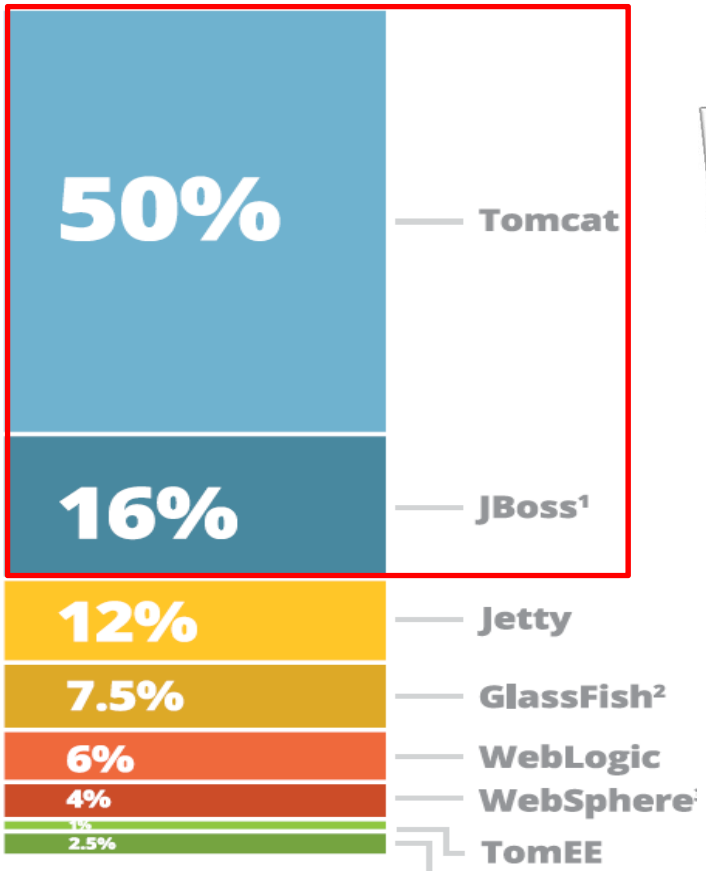
OWASP Top 10 2013

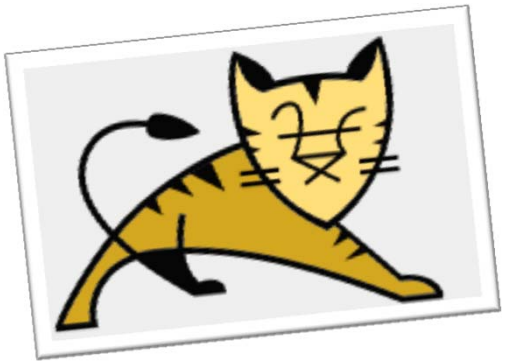
- 2013-A1 – Injection
- 2013-A2 – Broken Authentication and Session Management
- 2013-A3 – Cross Site Scripting (XSS)
- 2013-A4 – Insecure Direct Object References
- 2013-A5 – Security Misconfiguration
- 2013-A6 – Sensitive Data Exposure
- 2013-A7 – Missing Function Level Access Control
- 2013-A8 – Cross-Site 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

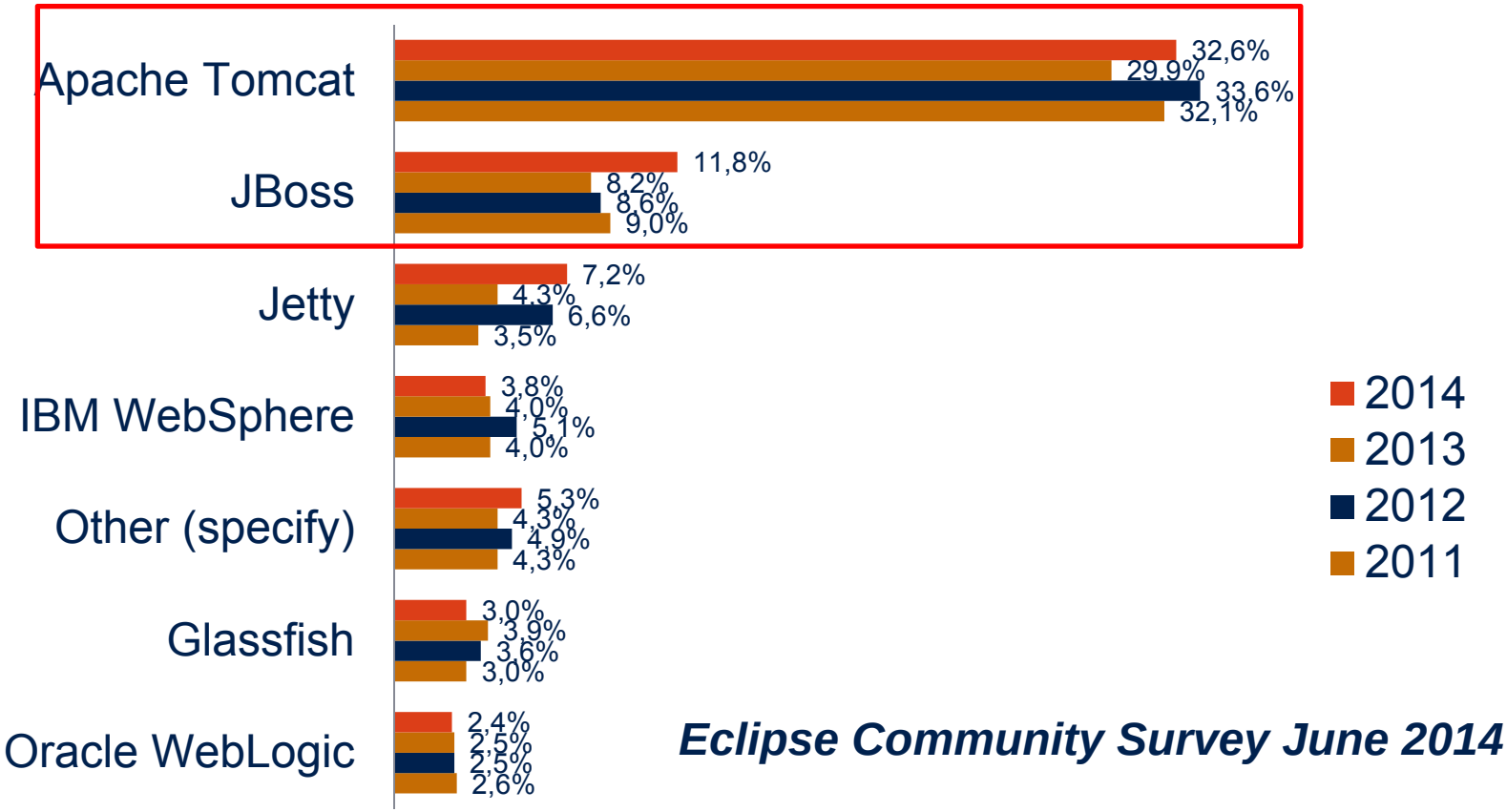
Welcher Anwendungsserver wird eingesetzt?





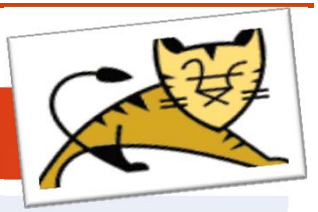
Java tools and technologies report 2014 RebelLabs

Welcher Anwendungsserver wird eingesetzt?



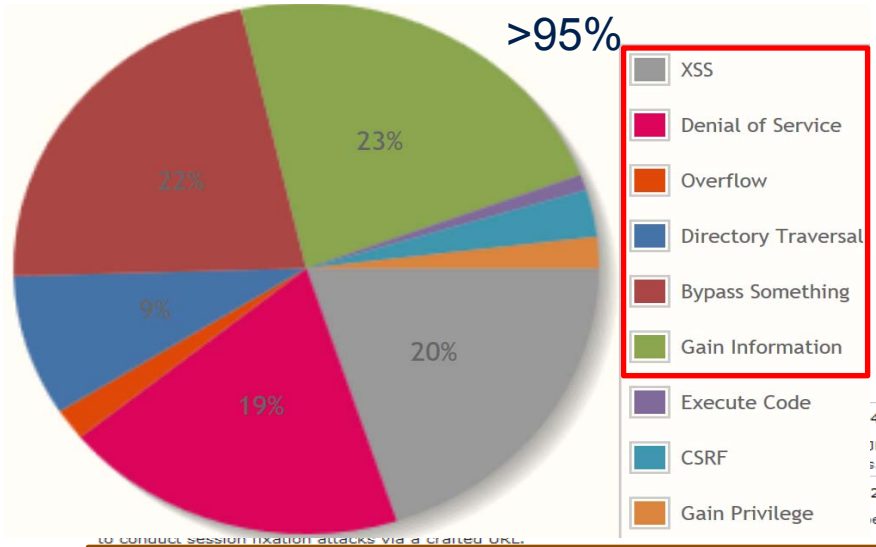
Eclipse Community Survey June 2014

Apache Tomcat Versionen



Veröffentlicht	Servlet/ JSP Spec		Tomcat Version	Java, EL Version
2013	**3.1**	**2.3**	**8.0.x (8.0.12)**	**JRE 1.7+(8), EL 3.0, TLS 1.2, JDBC 4.1**
2010	3.0	2.2	7.0.x **(7.0.55)**	JRE 1.6+**(8)**, EL 2.2, TLS 1.0, JDBC 4.0
2006	2.5	2.1	6.0.x **(6.0.41)**	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

Welche Tomcat-Schwachstellen? (cvedetails.com)



[ANN] Apache Tomcat Native 1.1.31 released
[ANN] Apache Tomcat 8.0.9 (stable) available
Re: [SECURITY] CVE-2014-0099 Apache Tomcat information disclosure
[SECURITY] CVE-2014-0119 Apache Tomcat information disclosure
[SECURITY] CVE-2014-0097 Apache Tomcat information disclosure
[SECURITY] CVE-2014-0096 Apache Tomcat information disclosure
[SECURITY] CVE-2014-0095 Apache Tomcat denial of service
[SECURITY] CVE-2014-0075 Apache Tomcat denial of service
[ANN] Apache Tomcat 7.0.54 released
[ANN] Apache Tomcat 6.0.41 released
[ANN] Apache Tomcat 8.0.8 (beta) available
[ANN] Apache Tomcat Connectors 1.2.40 released

				4-24		5.0	None	Remote	Low	Not required	None	None	Partial

JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU

				2-26		4.3	None	Remote	Medium	Not required	Partial	None	None

es not consider the disableURLRewriting setting when handling a session ID in a URL, which allows remote attackers

to conduct session fixation attacks via a crafted URL.

3	CVE-2013-6357	352	CSRF	2013-11-13	2013-11-14	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

** DISPUTED ** Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST method, as demonstrated by a /manager/html/undeploy?path= URI. NOTE: the vendor disputes the significance of this report, stating that "the Apache Tomcat Security team has not accepted any reports of CSRF attacks against the Manager application ... as they require a reckless system administrator."

4	CVE-2013-4590	200	+Info	2014-02-26	2014-02-26	4.3	None	Remote	Medium	Not required	Partial	None	None

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 allows attackers to obtain "Tomcat internals" information by leveraging the presence of an untrusted web application with a context.xml, web.xml, *.jspx, *.tagx, or *.tld XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

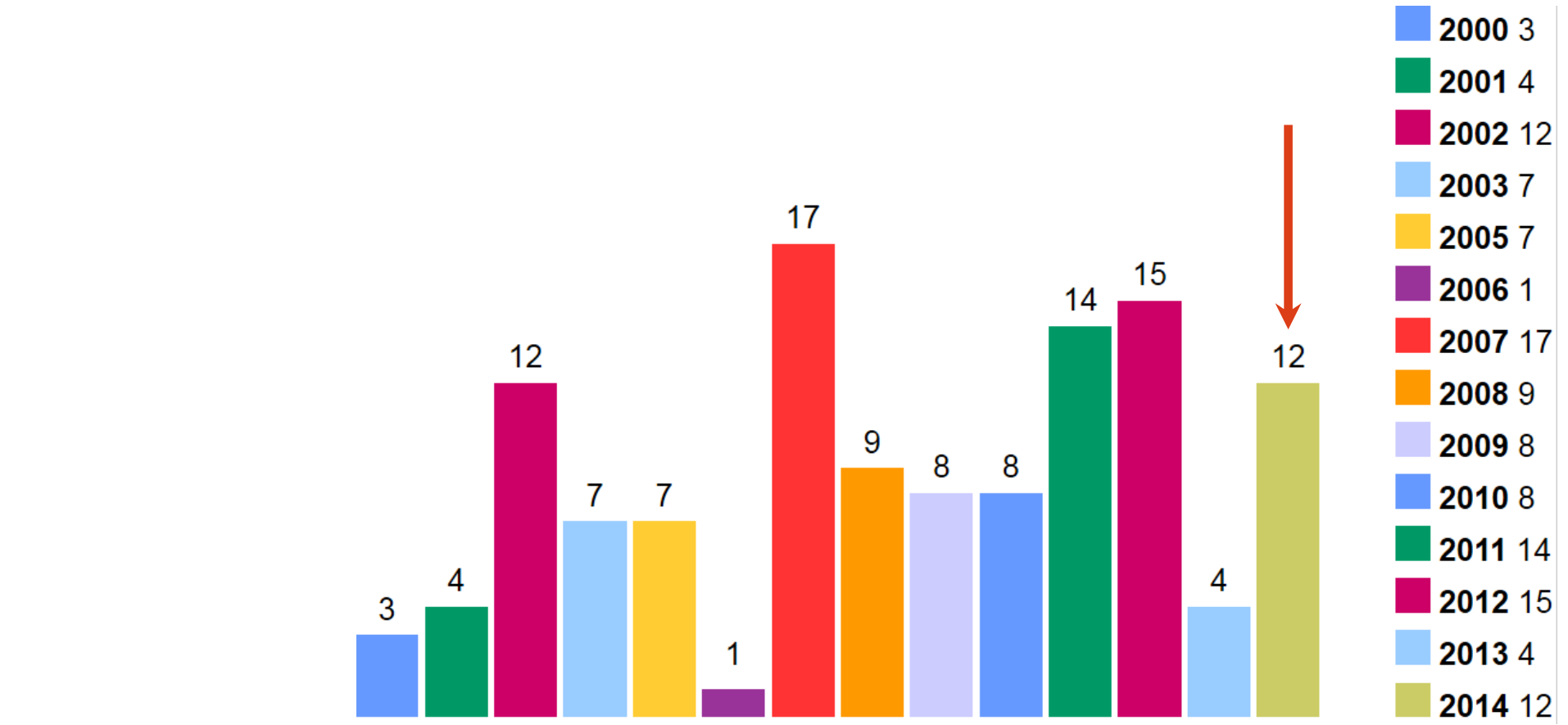
5	CVE-2013-4322	20	DoS	2014-02-26	2014-02-26	4.3	None	Remote	Medium	Not required	None	None	Partial

Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.

6	CVE-2013-4286	20		2014-02-26	2014-04-04	5.8	None	Remote	Medium	Not required	Partial	Partial	None

Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.

Entwicklung der Tomcat-Schwachstellen? (cvedetails.com)



http://tomcat.apache.org
http://tomcat.apache.org/security.html
http://tomcat.apache.org/tomcat-8.0-doc/security-howto
http://docs.oracle.com/javase/7/docs/technotes/guides/
http://www.mulesoft.com/improving-apache-tomcat-sec
https://www.owasp.org/index.php/Securing_tomcat
https://bugs.openjdk.java.net/browse/JDK

tomcat-dev mailing list archives

Site index · List index

Message view

From	bugzi...@apache.org
Subject	Bug report for Tomcat 8 [2014/02/09]
Date	Sun, 09 Feb 2014 07:15:43 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                                |   |
|     |   |   |          |                                            |   |
|51497|New|Enh|2011-07-11|Use canonical IPv6 text representation in logs    |
|53737|Opn|Enh|2012-08-18|Use ServletContext.getJspConfigDescriptor() in Jas|
|53930|New|Enh|2012-09-24|allow capture of catalina stdout/stderr to a comma|
|54503|New|Enh|2013-01-29|SAML2 based single sign on                        |
|54700|New|Enh|2013-03-15|Improvement: Add support for system property to sp|
|54741|New|Enh|2013-03-22|Add org.apache.catalina.startup.Tomcat#addWebapp(S|
|55006|New|Enh|2013-05-22|Add http proxy support for ClientEndpoint using sy|
|55243|New|Enh|2013-07-11|Add special search string for nested roles        |
|55252|New|Enh|2013-07-12|Separate Ant and command-line wrappers for JspC   |
|55383|New|Enh|2013-08-07|Improve markup and design of Tomcat's HTML pages  |
|55479|New|Enh|2013-08-24|JSR 196 (JASPIC) support in Tomcat                |
```

Fixed in Apache Tomcat 7.0.33

Important: Session fixation CVE-2013-2067

FORM authentication associates the most recent request requiring authent
login form, an attacker could inject a request that would be executed using

This was fixed in revision 1408044.

This issue was identified by the Tomcat security team on 15 Oct 2012 and

Affects: 7.0.0–7.0.32

bugzi...@apache.org	Bug report for Taglibs [2014/08/03]
bugzi...@apache.org	Bug report for Tomcat 6 [2014/08/03]
bugzi...@apache.org	Bug report for Tomcat 8 [2014/08/03]
bugzi...@apache.org	Bug report for Tomcat 7 [2014/08/03]
bugzi...@apache.org	Bug report for Tomcat Connectors [2014

Permalink (Message view)

From	bugzi...@apache.org
Subject	Bug report for Tomcat 8 [2014/08/03]
Date	Sun, 03 Aug 2014 07:16:14 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                                |   |
|     |   |   |          |                                            |   |
|43925|Opn|Enh|2007-11-21|org.apache.jasper.runtime.BodyContentImpl causing
|51497|New|Enh|2011-07-11|Use canonical IPv6 text representation in logs    |
|53737|Opn|Enh|2012-08-18|Use ServletContext.getJspConfigDescriptor() in Jas|
|53930|New|Enh|2012-09-24|allow capture of catalina stdout/stderr to a comma|
|54503|New|Enh|2013-01-29|SAML2 based single sign on                        |
|54700|New|Enh|2013-03-15|Improvement: Add support for system property to sp|
|54741|New|Enh|2013-03-22|Add org.apache.catalina.startup.Tomcat#addWebapp(S|
|55006|New|Enh|2013-05-22|Add http proxy support for ClientEndpoint using sy|
|55243|New|Enh|2013-07-11|Add special search string for nested roles        |
|55252|New|Enh|2013-07-12|Separate Ant and command-line wrappers for JspC   |
|55383|New|Enh|2013-08-07|Improve markup and design of Tomcat's HTML pages  |
|55479|New|Enh|2013-08-24|JSR 196 (JASPIC) support in Tomcat                |
|55559|New|Enh|2013-09-14|UserDatabaseRealm enhacement: may use local JNDI  |
|55675|New|Enh|2013-10-18|Checking and handling invalid configuration option|
|55770|New|Enh|2013-11-12|Allow the crlFile to be reloaded                  |
|55788|New|Enh|2013-11-16|TagPlugins should key on tag QName rather than imp|
|55884|Ver|Maj|2013-12-14|JSPs no longer compile in Java 8                  |
```

via XXE when running untrusted web applications
-2012-3544 (Denial of Service)
-2005-2090 (Information disclosure)
ssible with disableURLRewriting enabled

Upload and Apache Tomcat DoS

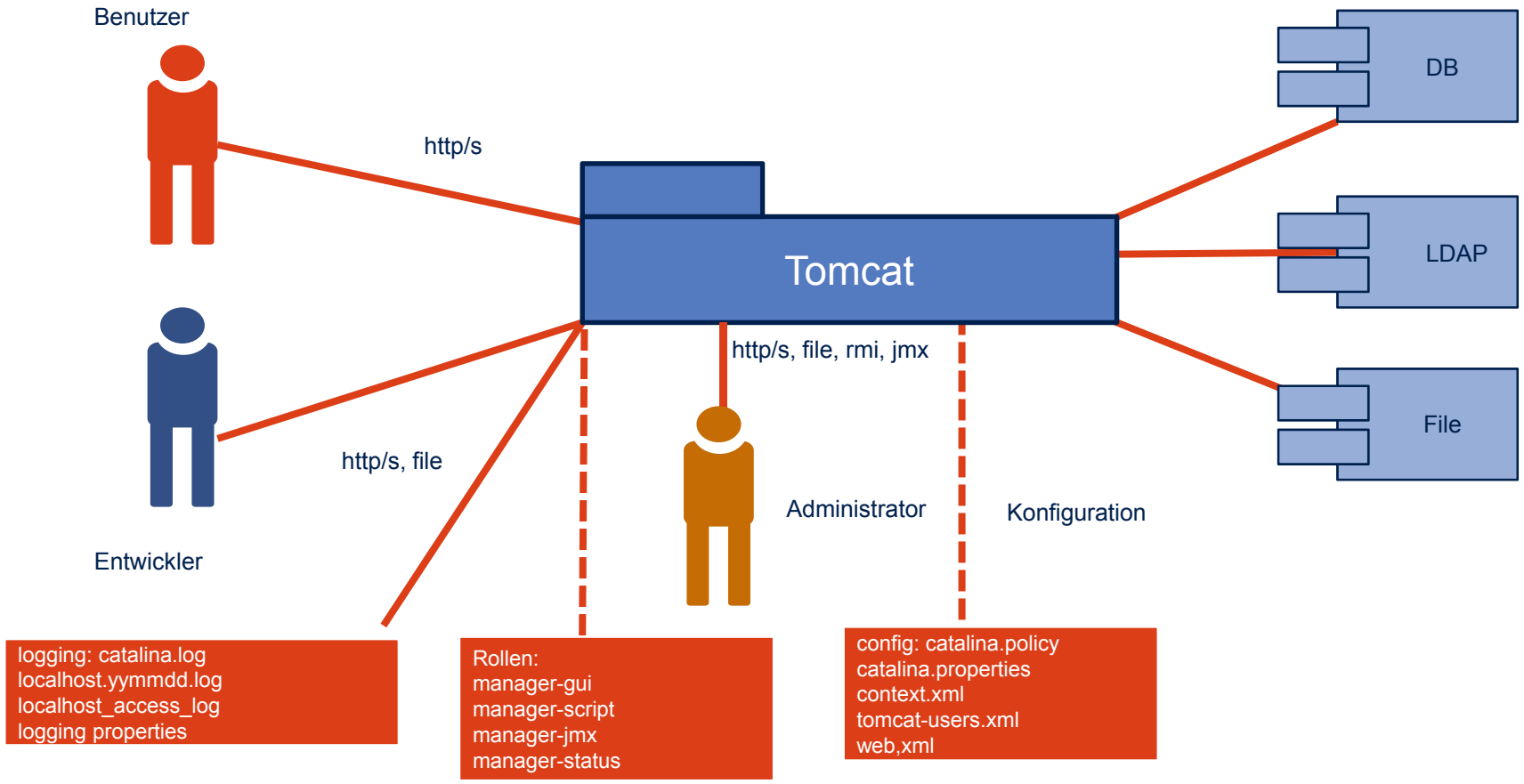
oding extension size is not limited
ORM authenticator
T authentication weaknesses
of Service

Release Date: 2015-01-19
Release Date: 2015-01-19
Release Date: 2014-10-13
Release Date: 2014-10-13
Release Date: 2014-10-13
Release Date: 2014-10-13

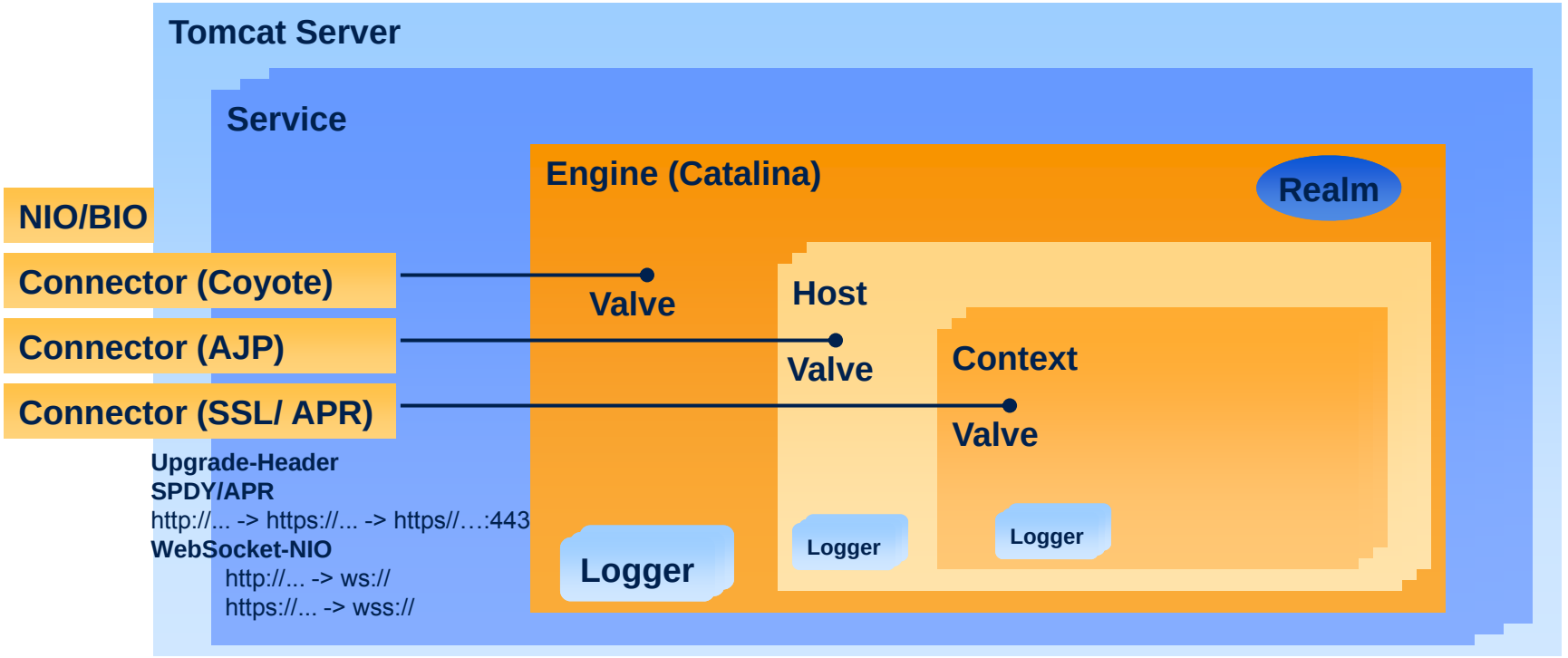
d 21 Nov 2012

completing the

Tomcat-Überblick: Sicherheits-Kontext

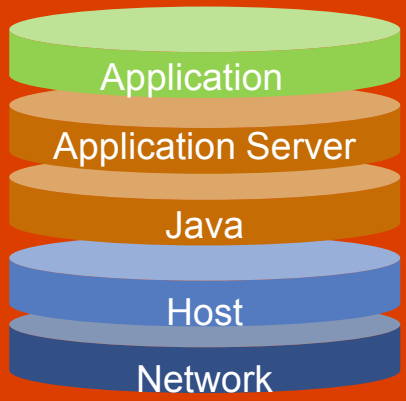


Tomcat Komponenten



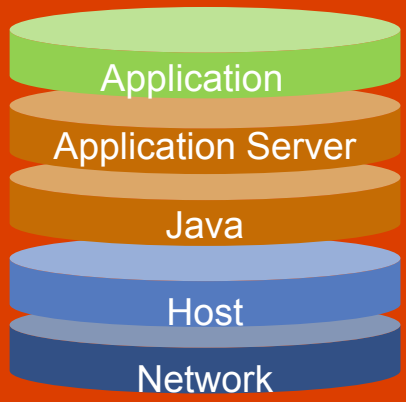
Sicherheit - aber wie?

- Ebenen der Sicherheit
- CVE-Bedrohungsarten, OWASP-Kategorien kennen
- Verschlüsselung, Chiffren, Algorithmen, Zertifikate
- Java, Policy, JCA, lange Schlüssel
- Authentifizierung, Autorisierung, Passwort Hashing
- Konfiguration abspecken (Tarnen, Fläche verkleinern, entfernen)
- Filtern (CsrfPreventionFilter, RemoteAddrValve)
- Aktualisierung ALLER Komponenten



Wie überwachen?

- JMX → Ressourcen-Verbrauch, Grenzwerte
- Logdateien → auswerten Auffälligkeiten, Fehlercodes
- Manager Console → Konfiguration, Ressourcen, Anwendungen
- Jar-Versionen überprüfen → CVEchecker, CVE Dependency-Check
- SSL/TLS ciphersuites anzeigen, überprüfen → cipherscan



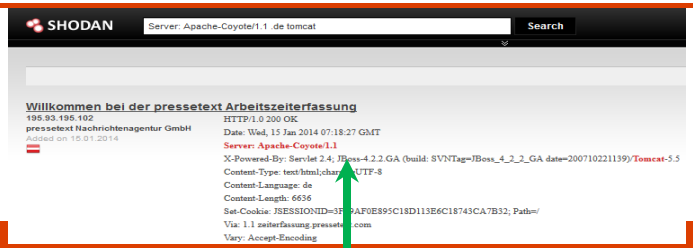
Sicherheit von Anfang an - abspecken

- Installationsdatei verifizieren

```
md5sum -c apache-tomcat-8.0.8.zip.md5
```

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

Tarnen, täuschen - Produktversion verschleiern



CATALINA_HOME/lib

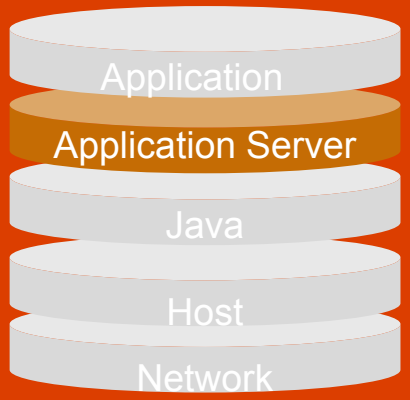
```
jar xf catalina.jar
org/apache/catalina/util/ServerInfo.properties
ServerInfo.properties server.info=Apache
server.number=0.0.0.0
jar uf catalina.jar
org/apache/catalina/util/ServerInfo.properties
```

CATALINA_HOME/conf/server.xml

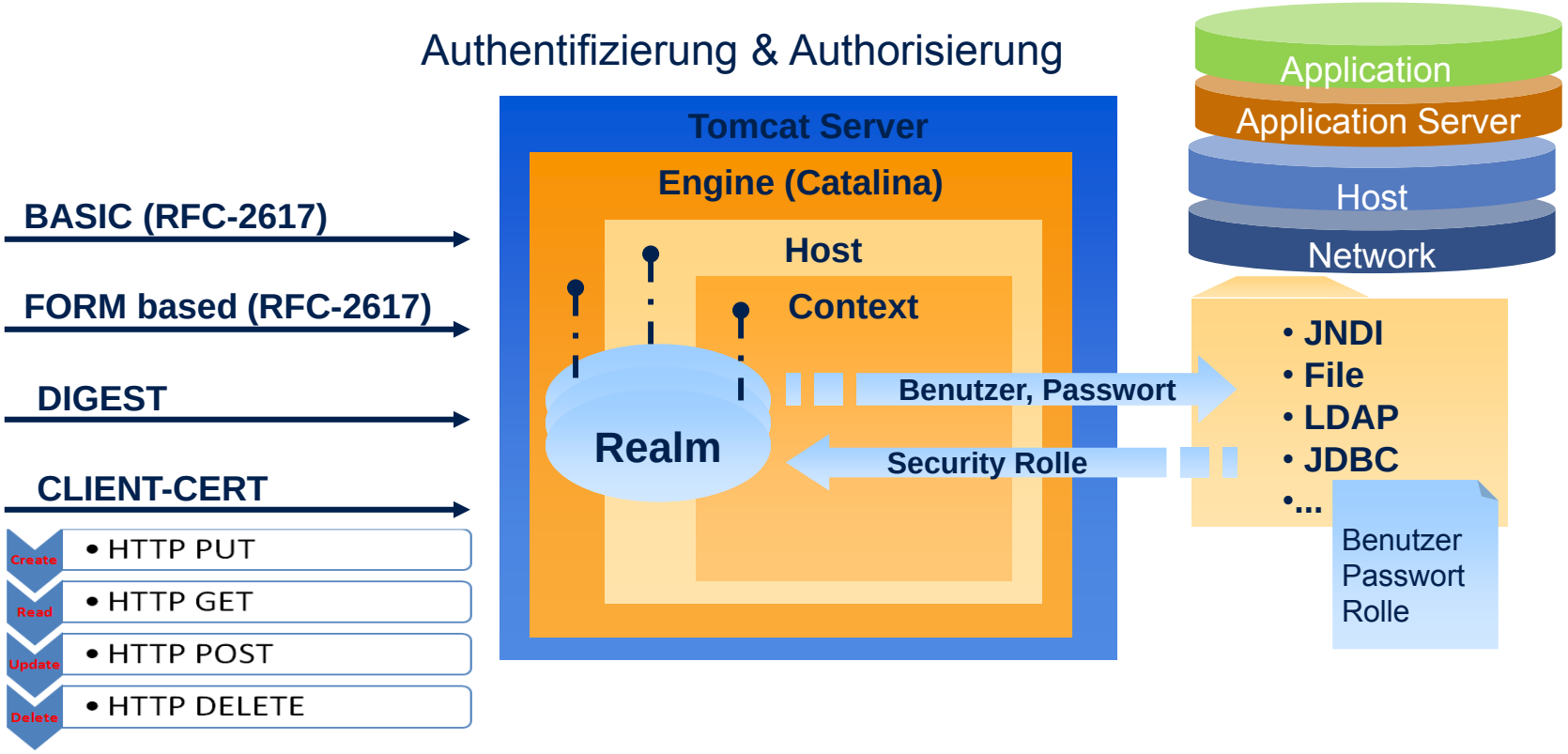
```
<Connector port="8080" ... server="Apache" />
```

Testen: version.[sh|bat]

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



Zugriff für Webanwendungen kontrollieren: Wer, Wie , Was?



2013-A2 Broken Authentication: Verschlüsselte Passwörter gestern & heute

"THEY WERE WAY AHEAD OF US IN PASSWORDS."

OWASP Top 10 für Entwickler-2013: A8 Cross-Site Request Forgery

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

Bedrohungs-quelle	Angriffs-vektor	Schwachstellen		Technische Auswirkung	Auswirkung auf das Unternehmen
———	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
- **JSF 2.2**
  - HTTP POST: **javax.faces.ViewState** hidden field with random token
  - HTTP GET **protected-views** in WEB-INF/faces-config.xml
  - URLs have the new **javax.faces.Token** URL parameter
- **< JSF 2.2**
  - **org.owasp.csrfguard.CsrfGuardFilter** 3.0

XSS-Angriffe: JSESSIONID als HttpOnly in Cookie statt URL zeitbegrenzt

Seit **Servlet 3.0 WEB-INF/web.xml**

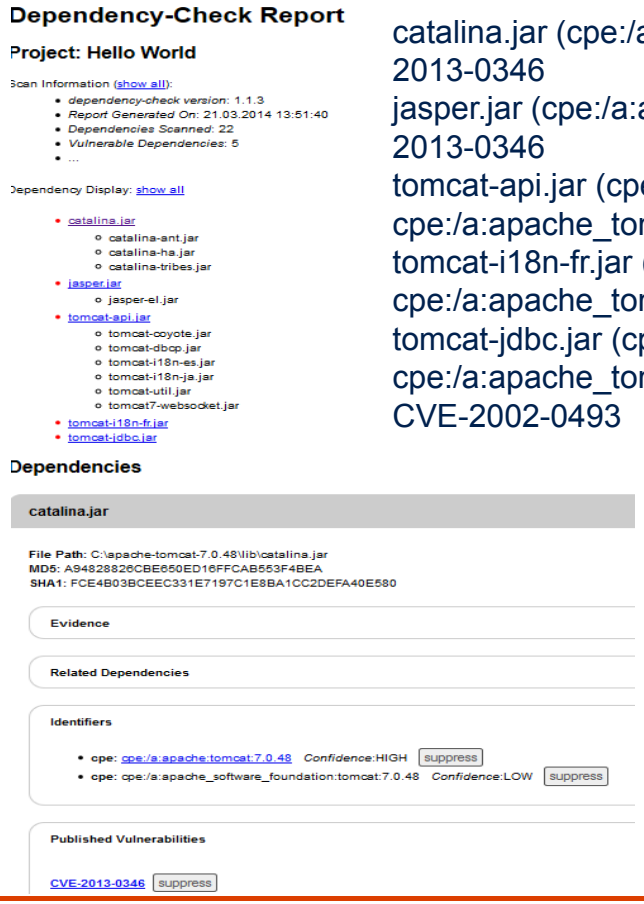
```
<session-config>
    <session-timeout>30</session-timeout>
    <cookie-config>
      <http-only>true</http-only>
    </cookie-config>
    <tracking-mode>COOKIE</tracking-mode>
</session-config>
```

Tomcat 6 in **CATALINA_BASE/conf/context.xml**, ab Tomcat 7 default

```
<?xml version="1.0" encoding="UTF-8"?>
<Context path="/myWebApplicationPath" useHttpOnly="true">
```

HTTP Strict Transport Security (***HSTS***) (**RFC 6797**) **Bug 54618**

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

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

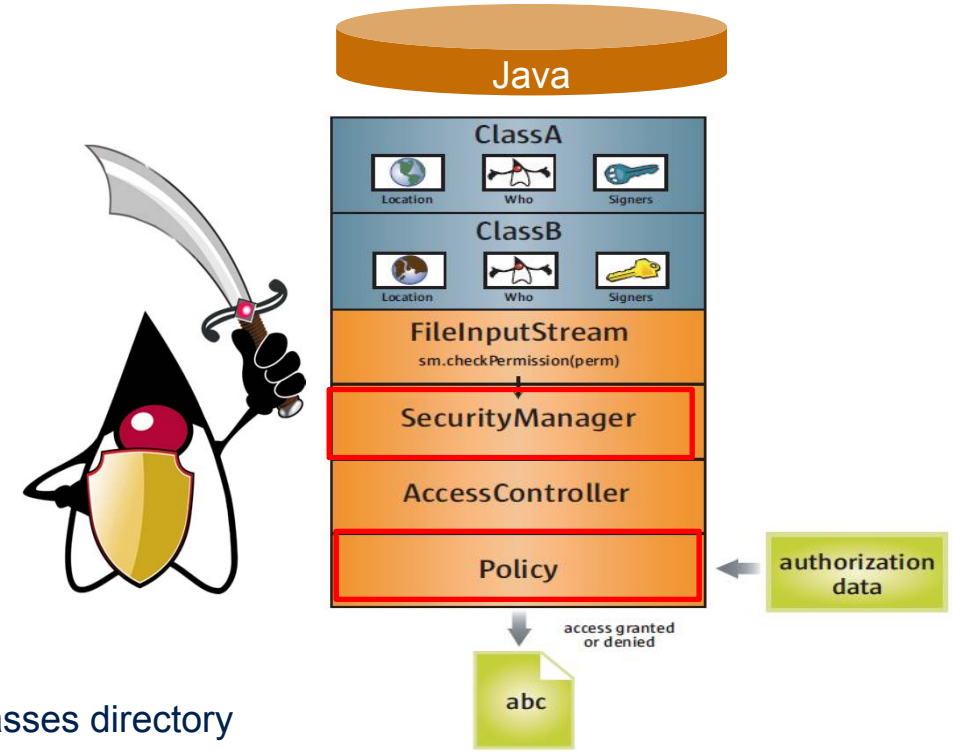
CVE-2013-0346 suppress

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

Java-Policies anwenden

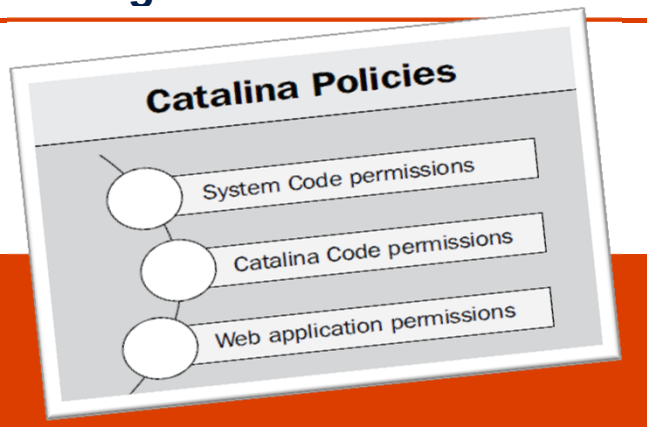
conf

- 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`

TLS 1.2 erste Wahl – seit 2008 bis heute

Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG
für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung

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

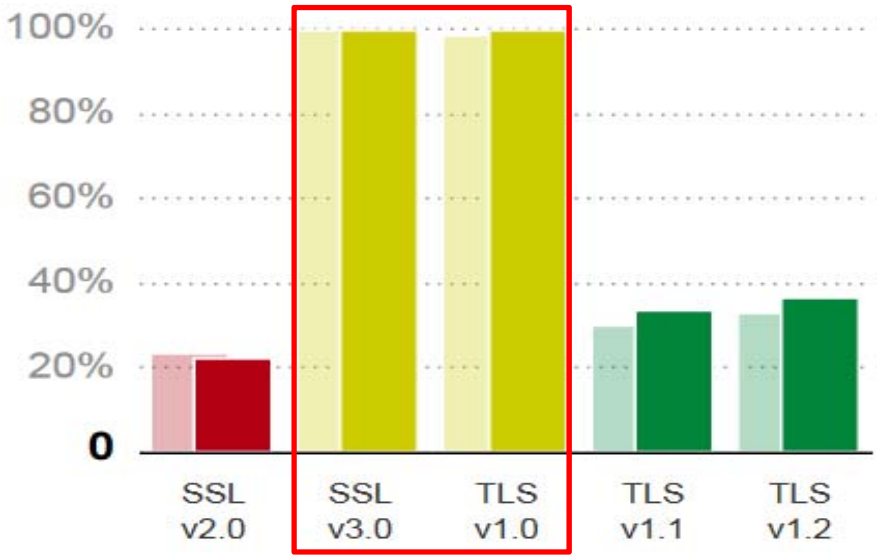
Ein "Mindeststandard" muss nicht das sein, was der Begriff nahelegt. Wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine solche Norm definiert, dann handelt es sich zunächst um eine "unverbindliche Empfehlung". So steht es auch mit dem jetzt verlangten Einsatz von TLS 1.2 als Transportverschlüsselung 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.

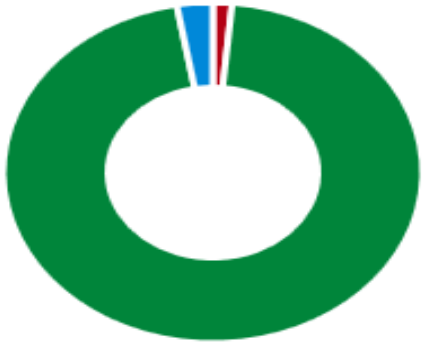
Bislang unterstützen Opera, Chrome 30 und der Internet Explorer von Microsoft TLS 1.2. Dort muss der Nutzer es jedoch teilweise erst aktivieren. Die Firefox-Entwickler arbeiten seit längerer Zeit daran, Safari auf Mac OS X nutzt immer noch TLS 1.0. Die iOS-Version des Browsers hingegen nutzt Version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

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

Protocol Support April/Mai 2014



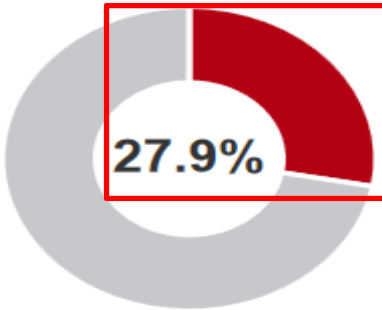
Key Strength Distribution Ciphers weaker than 128 bits



Below 2048 bits
567 0.4%
- 0.2 %

2048 bits
151,010 96.8%
+ 0.0 %

4096 bits
4,345 2.8%
+ 0.3 %



Sites that support weak or insecure cipher suites
43,561
- 1.1 %

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, SHA1, DSA, RSA keySize < 2048

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

Java Cryptography Architecture Standard Algorithm Name Documentation for JDK 8

Standard Algorithm Name Documentation

docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#SecureRandom

	• PBEWithHmacSHA1AndDESede (PKCS #5, 2.0) Note: These all use only the low order 8 bits of each password character.
PBKDF2With<*prf*>	Password-based key-derivation algorithm found in PKCS #5 2.0 using the specified pseudo-random function (<*prf*>). Example: PBKDF2WithHmacSHA256.

`SecureRandom` Number Generation Algorithms

The algorithm name in this section can be specified when generating an instance of `SecureRandom`.

Algorithm Name	Description
NativePRNG	Obtains random numbers from the underlying native OS. No assertions are made as to the blocking nature of generating these numbers.
NativePRNGBlocking	Obtains random numbers from the underlying native OS, blocking if necessary. For example, `/dev/random` on UNIX-like systems.
NativePRNGNonBlocking	Obtains random numbers from the underlying native OS, without blocking to prevent applications from excessive stalling. For example, `/dev/urandom` on UNIX-like systems.
PKCS11	Obtains random numbers from the underlying installed and configured PKCS11 library.
SHA1PRNG	The name of the pseudo-random number generation (PRNG) algorithm supplied by the SUN provider. This algorithm uses SHA-1 as the foundation of the PRNG. It computes the SHA-1 hash over a true-random seed value concatenated with a 64-bit counter which is incremented by 1 for each operation. From the 160-bit SHA-1 output, only 64 bits are used.
Windows-PRNG	Obtains random numbers from the underlying Windows OS.

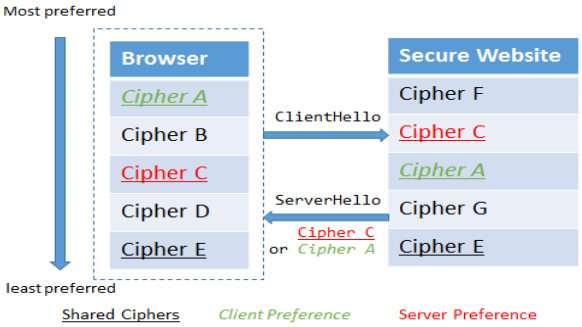
- `Mac` Algorithms
- `MessageDigest` Algorithms
- `Policy` Types
- `SaslClient` Mechanisms
- `SaslServer` Mechanisms
- `SecretKeyFactory` Algorithms
- `SecureRandom` Number Generation (RNG) Algorithms
- Service Attributes
- `Signature` Algorithms
- `SSLContext` Algorithms
- `TrustManagerFactory` Algorithms
- XML Signature (`XMLSignatureFactory`/`KeyInfoFactory`/`TransformService`) Mechanisms
- XML Signature Transform (`TransformService`) Algorithms
- JSSE Cipher Suite Names

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*

Schwache Chiffren & SSL 2.0 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=„TLSv1.2" 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"/>

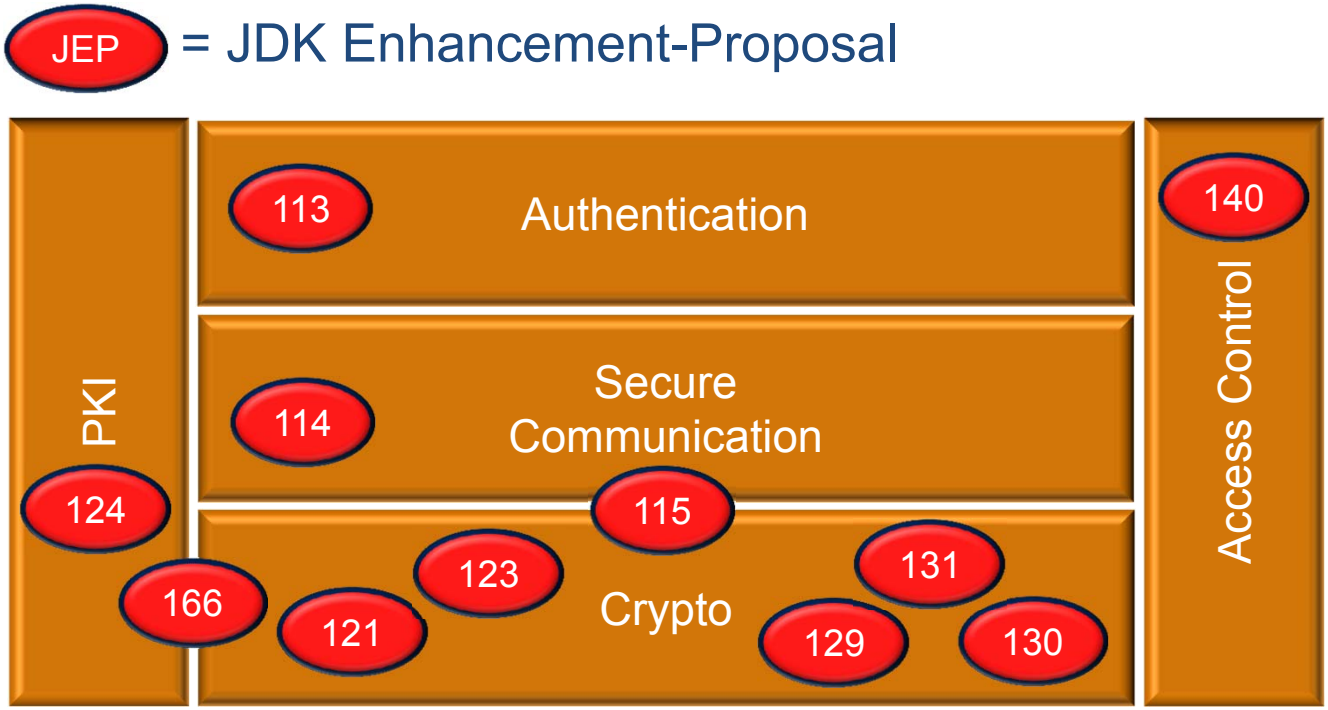
java -Djavax.net.debug=help MyApp

<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" sslProtocol="TLS" />

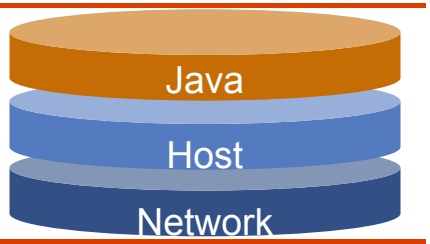
Sicherheitsneuerungen in Java 8

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**

Bereiche der Sicherheitsneuerungen in Java 8



Secure Sockets Layer (SSL) mit Tomcat auf zwei Wegen



Zwei Konnektoren:

1. **JSSE** protocol="org.apache.coyote.http11.**Http11NioProtocol**“ (**TLS 1.x**)
2. **OpenSSL** 1.0.1h/i (Bug 56844)-> **1.1.31, APR 1.5.1** protocol="org.apache.coyote.http11.**Http11AprProtocol**“ (nur **TLS 1.0**, Bug 53952 support TLS 1.1 & 1.2)

Zwei Keystore-Formate:

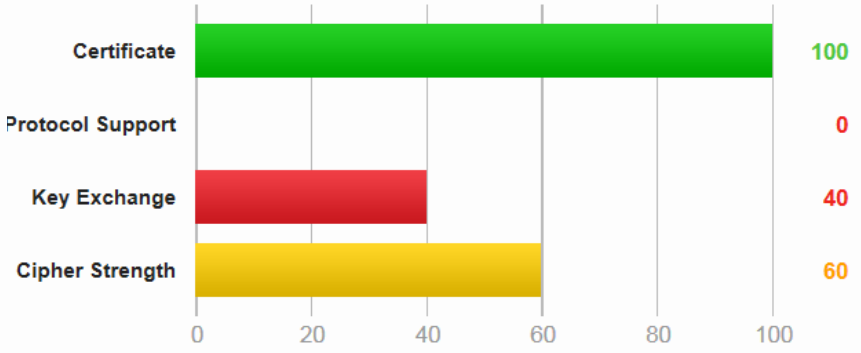
- **JKS** (Java KeyStore): java **keytool**
- **PKCS12** (Public Key Cryptography Personal Information Exchange Syntax): **OpenSSL**

SSL Report: datenabgabe.dpma.de (194.59.120.31)

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

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

SSL_CK_RC4_128_EXPORT40_WITH_MD5 (0x20080) **INSECURE**	40
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **WEAK**	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) FS **WEAK**	40
SSL_CK_DES_64_CBC_WITH_MD5 (0x60040) **INSECURE**	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	56
SSL_CK_RC4_128_WITH_MD5 (0x10080) **INSECURE**	128
SSL_CK_RC2_128_CBC_WITH_MD5 (0x30080) **INSECURE**	128



Best Practices, SSL Server Rating Guide, OpenSSL Cookbook and known issues.

orts SSL 2, which is obsolete and insecure. Grade set to F.

does not mitigate the CRIME attack. Grade capped to B.

to the OpenSSL CCS vulnerability (CVE-2014-0224), but probably not exploitable

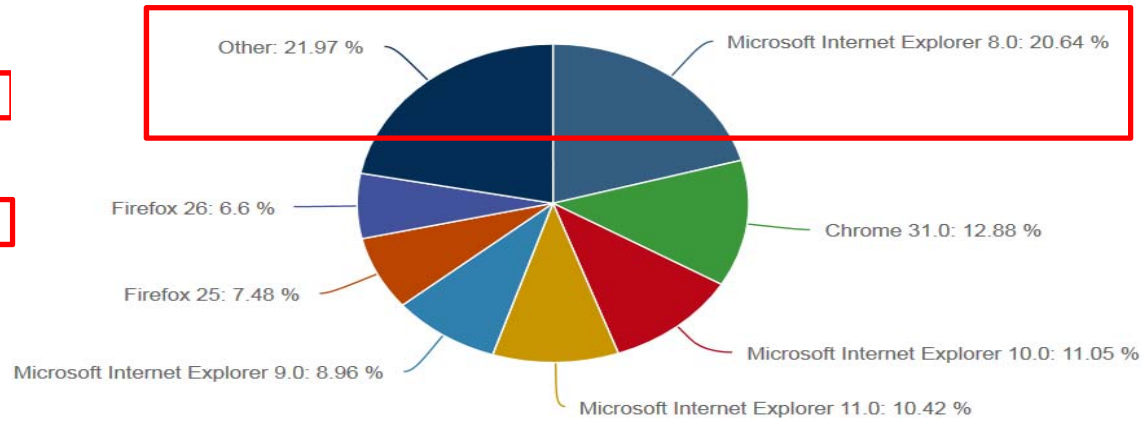
The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

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

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	Platforms	TLS 1.0	TLS 1.1	TLS 1.2
Google Chrome [notes 2] [notes 3]	0–21	Android, iOS, Linux, Mac OS X, Windows (XP, Vista, 7, 8)	Yes	No	No
	22–29		Yes[33]	Yes	No[33][34][35][36]
	30–		Yes[33]	Yes[33]	Yes[34][35][36]
Mozilla Firefox [notes 3] [notes 4]	1–22 ESR 10, 17	Android, Firefox OS, Linux, Mac OS X, Windows (XP, Vista, 7, 8)	Yes[37]	No[29]	No[31]
	23		Yes[37]	Yes, disabled by default[29][38]	No[31]
	24–26 ESR 24		Yes[37]	Yes, disabled by default[29][38]	Yes, disabled by default[31]
	27–		Yes[37]	Yes[29][38][40]	Yes[31][39][40]
Internet Explorer [notes 5]	6	Windows (98, 2000, ME, XP)	Yes, disabled by default	No	No
	7–8	Windows XP	Yes	No	No
	7–9	Windows Vista	Yes	No	No
	8–10	Windows 7	Yes	Yes, disabled by default	Yes, disabled by default
	10	Windows 8	Yes	Yes, disabled by default	Yes, disabled by default
	11	Windows 7, 8.1	Yes	Yes[43]	Yes[43]

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

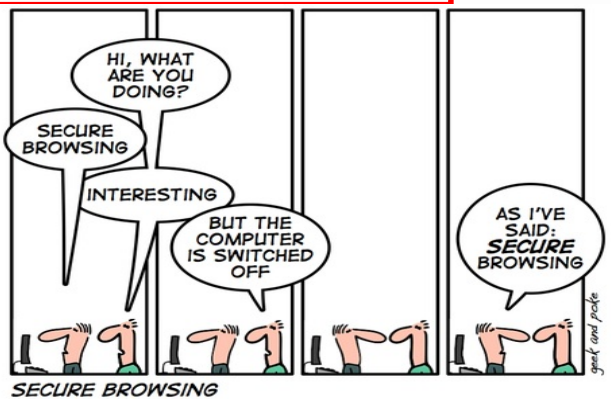
(*) This test reliably detects only the highest supported protocol.

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+



Fazit: Apache Tomcat aber sicher!

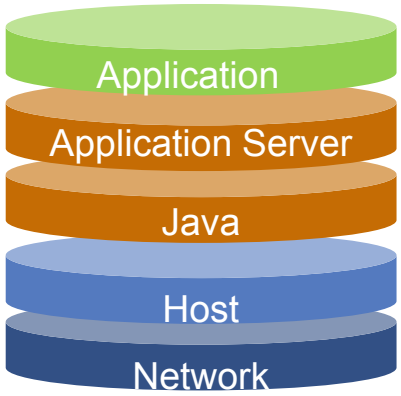
- Wie groß ist die Bedrohung?
- Ist SSL wirklich sicher?
- Tomcat ist bedroht!
- Sicherheit von Anfang an: default is faul(t)
- Mehrstufige Verteidungsstrategie!
- Der Weg ist das Ziel

Sind Sie sicher?

Muss ich das jetzt auch noch tun …

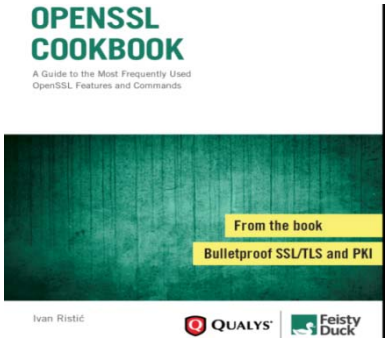
Ausblick – Kryptokalypse?

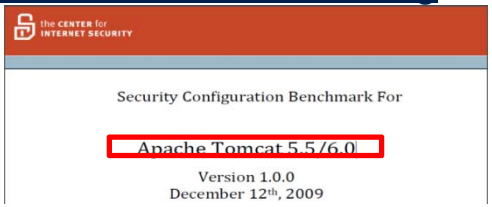
- **2014 ~~wird~~ IST das Jahr der Kryptographie**
- TLS 1.2 **ist sicher**, wenn Client&Server **korrekt eingestellt!**
- **Clients** hinken bei Sicherheit **Server** hinterher
- **Sicherheit kostet!** (Zeit&Geld&Performance → Ruf)
- **Kenne deine** Systeme, Angreifer und Waffen!



Weitere Infos

- **Tomcat 8 Dokumentation**
  - http://tomcat.apache.org/tomcat-80-doc/security-howto.html, http://wiki.apache.org/tomcatq/FAQ/Security
- **OWASP-Empfehlungen für Tomcat**
  - https://www.owasp.org/index.php/Securing_tomcat
- **SSL/TLS Deployment Best Practices**, Ivan Ristić, v1.3, 2013
- https://wiki.mozilla.org/Security/Server_Side_TLS
- http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#Debug
- **BSI Sicherheitsuntersuchung** des Apache Jakarta Tomcat, 2006
- **CIS Apache Tomcat** 5.5/6.x Server Security Benchmark v1.0.0, 2009
- **Tomact aber sicher**, Frank Pientka, **JavaSpektrum 04/2014**





1. – 4. September 2014
in Nürnberg

Herbstcampus

Wissenstransfer
par excellence

Vielen Dank!

Frank Pientka
Materna GmbH