MATERNA
Information & Communications

# Apache Tomcat aber sicher!

***Frank Pientka, Dortmund***

# Wer ist Materna?



Dr. Winfried Materna

Helmut an de Meulen

Gründer

**Gegründet 1980**

**1.400 Mitarbeiter**

**Umsatz 2013:**
**158 Mio. €**

# Vorstellung des Referenten: Frank Pientka


Dipl.-Informatiker (TH Karlsruhe)

Software Architect in Dortmund

iSAQB-Gründungsmitglied

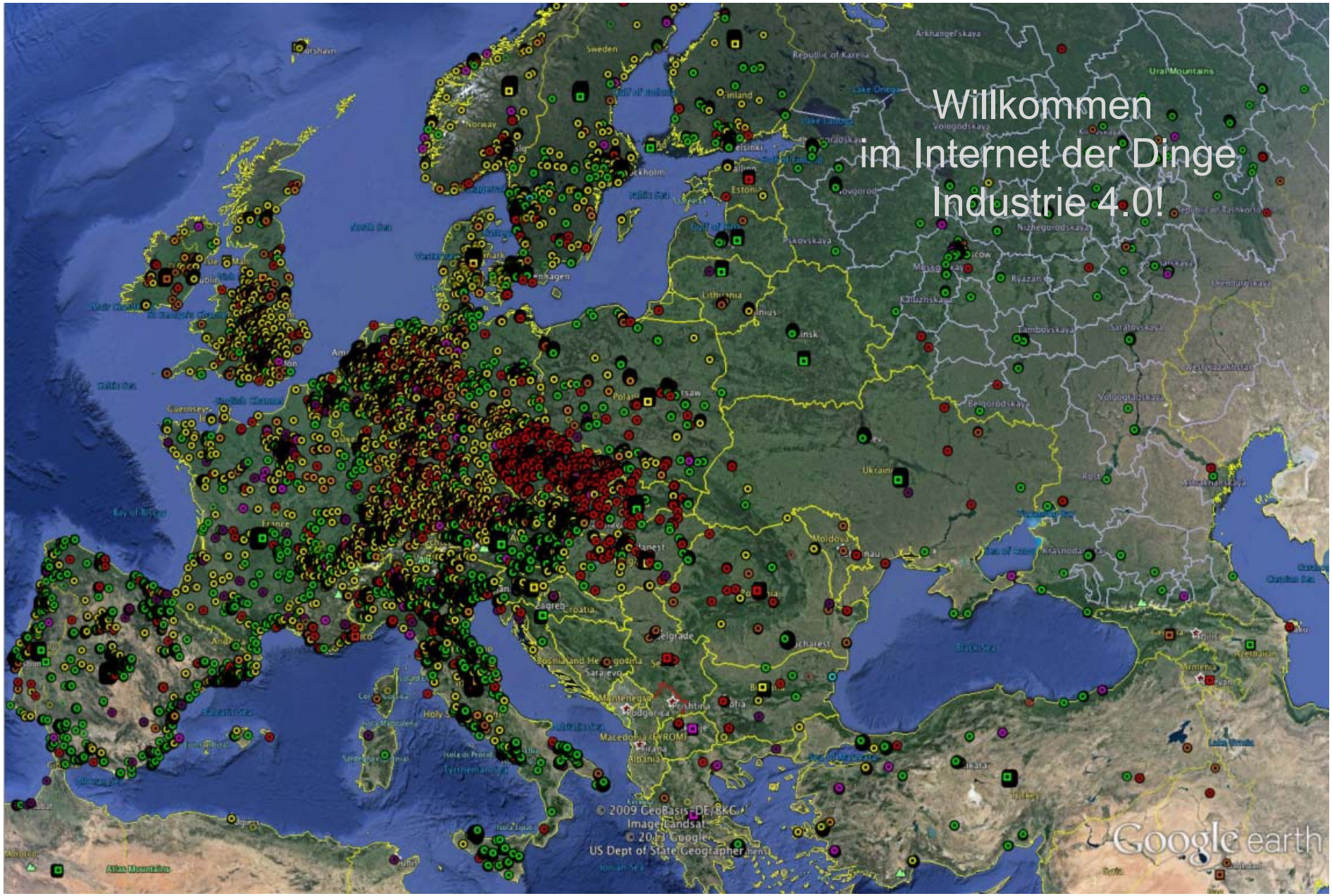
heise.de/developer/Federlesen-Kolumne

Über 20 Jahre IT-Erfahrung
Veröffentlichungen und Vorträge zu:

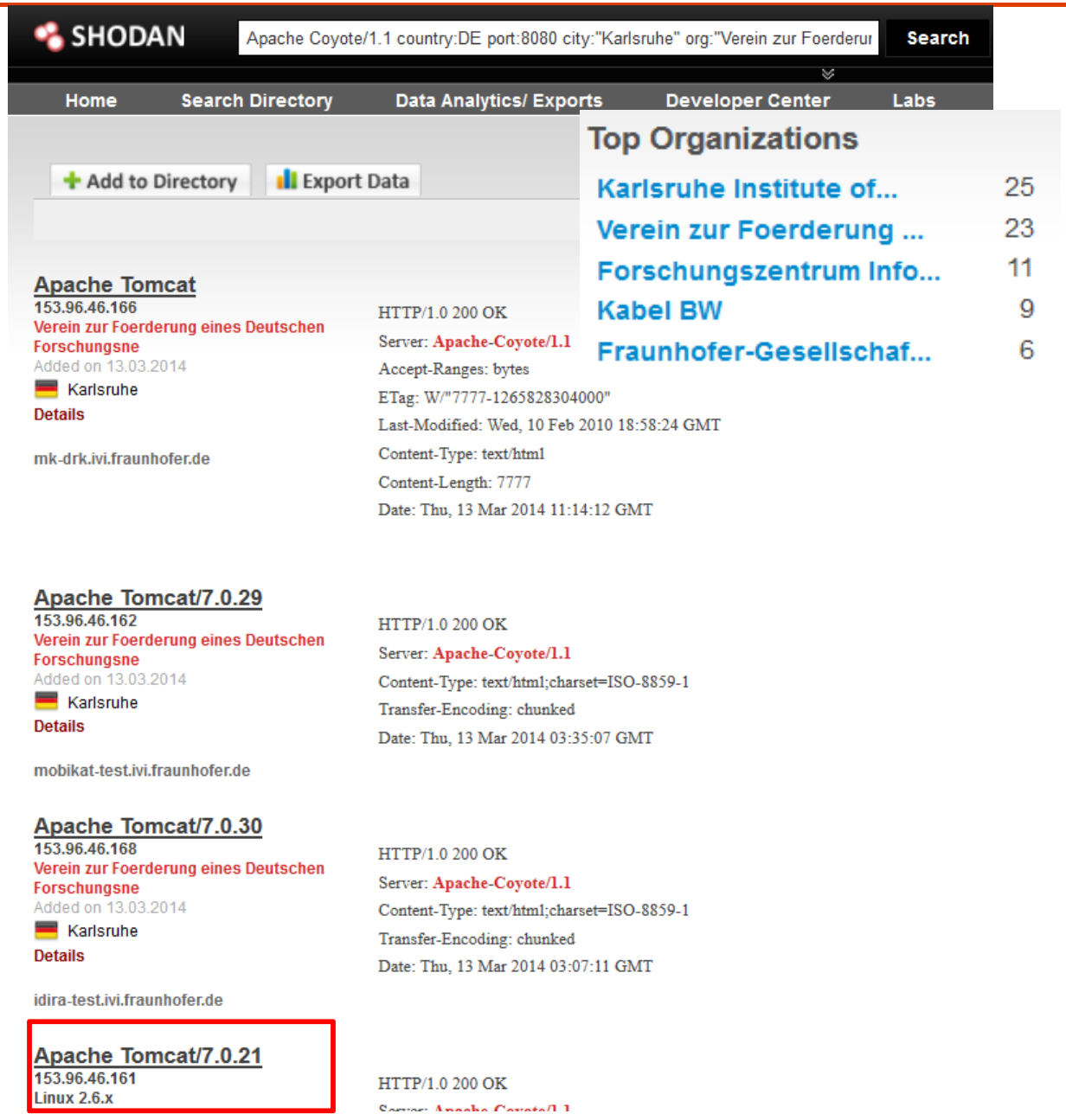
**Datenbanken, Applikations- und Portalservern**

# Sicherheitslücke im Herzen des Internets 8.April 2014

# Freier Zugriff auf Fernsteuerungen für Industrieanlagen (FU Berlin 24.02.2014)



# http://www.shodanhq.com/search?q=Apache+Coyote%2F1.1+country%3ADE+port%3A8080+city%3A%22Karlsruhe%22+tomcat



# 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

# DoS mit demTomcat-Wurm Java.Tomdep

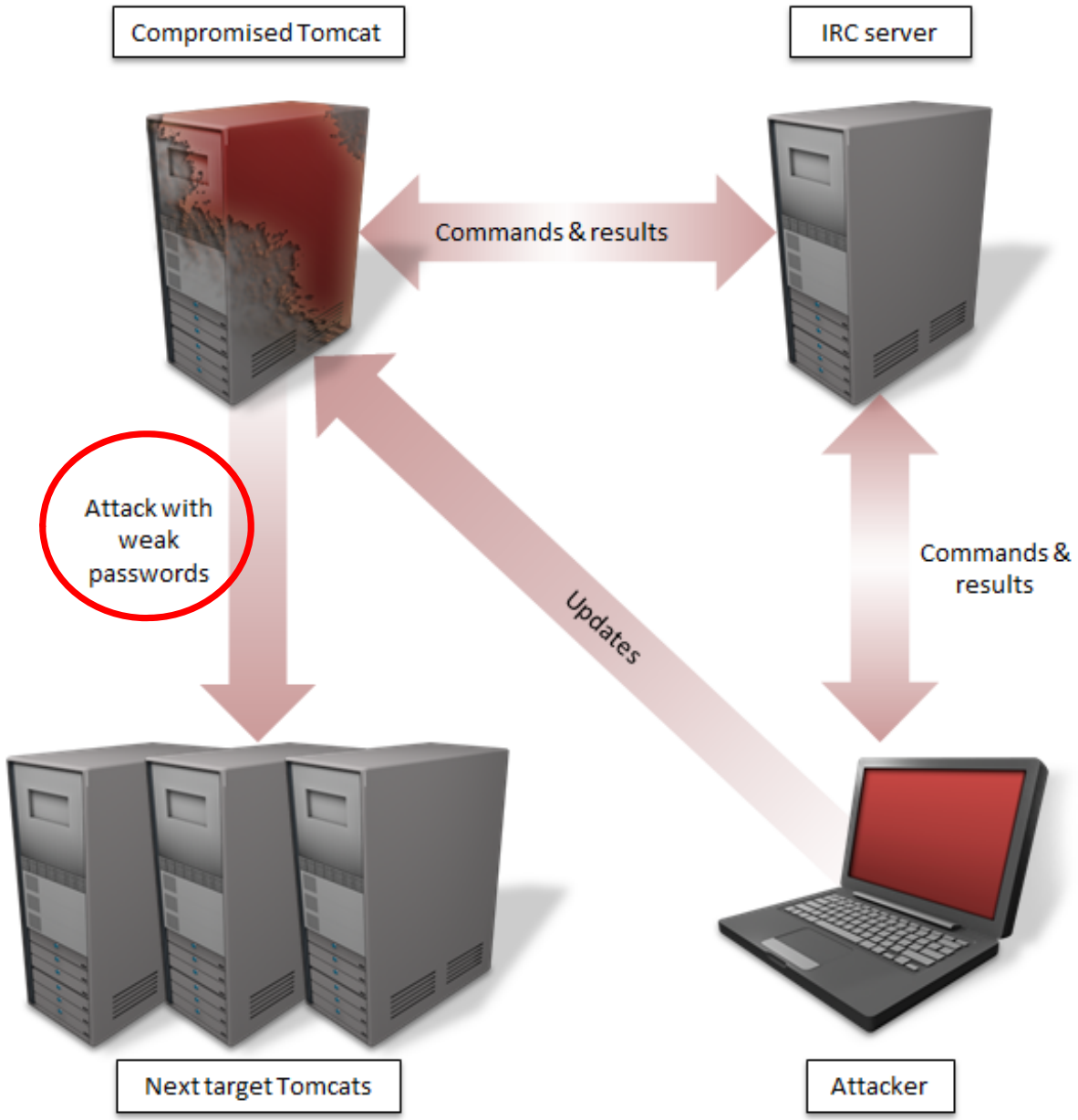
JAVA.TOMDEP

## Backdoor-Wurm greift Tomcat-S

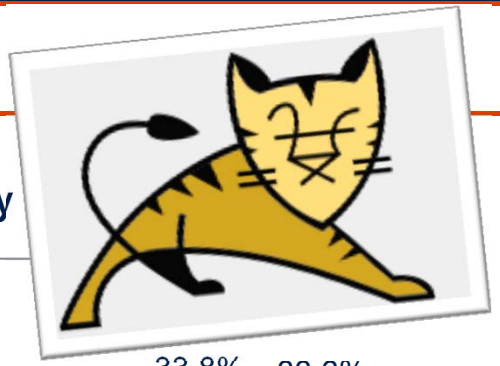
Symantec hat einen neuen Wurm entdeckt, der sich s
weiterverbreitet und auf infizierten Systemen eine Ba
Allerdings greift Java.Tomdep nicht normale PCs an, s

Java.Tomdep sei eine durchaus ungewöhnliche Erscheinung
Symantec Sicherheitsforscher in einem Blogeintrag : Der W
wie viele, verbreitet sich von infizierten Systemen aus weite
Backdoor und kann von den Angreifern per IRC-Server geste
Dennoch gibt es bei Java-Tompdep einen kleinen Unterschie
sich um ein Java-Servlet, das sich von Server zu Server verbr
Server-Würmer seien bislang vor allen in PHP aufgefallen, s

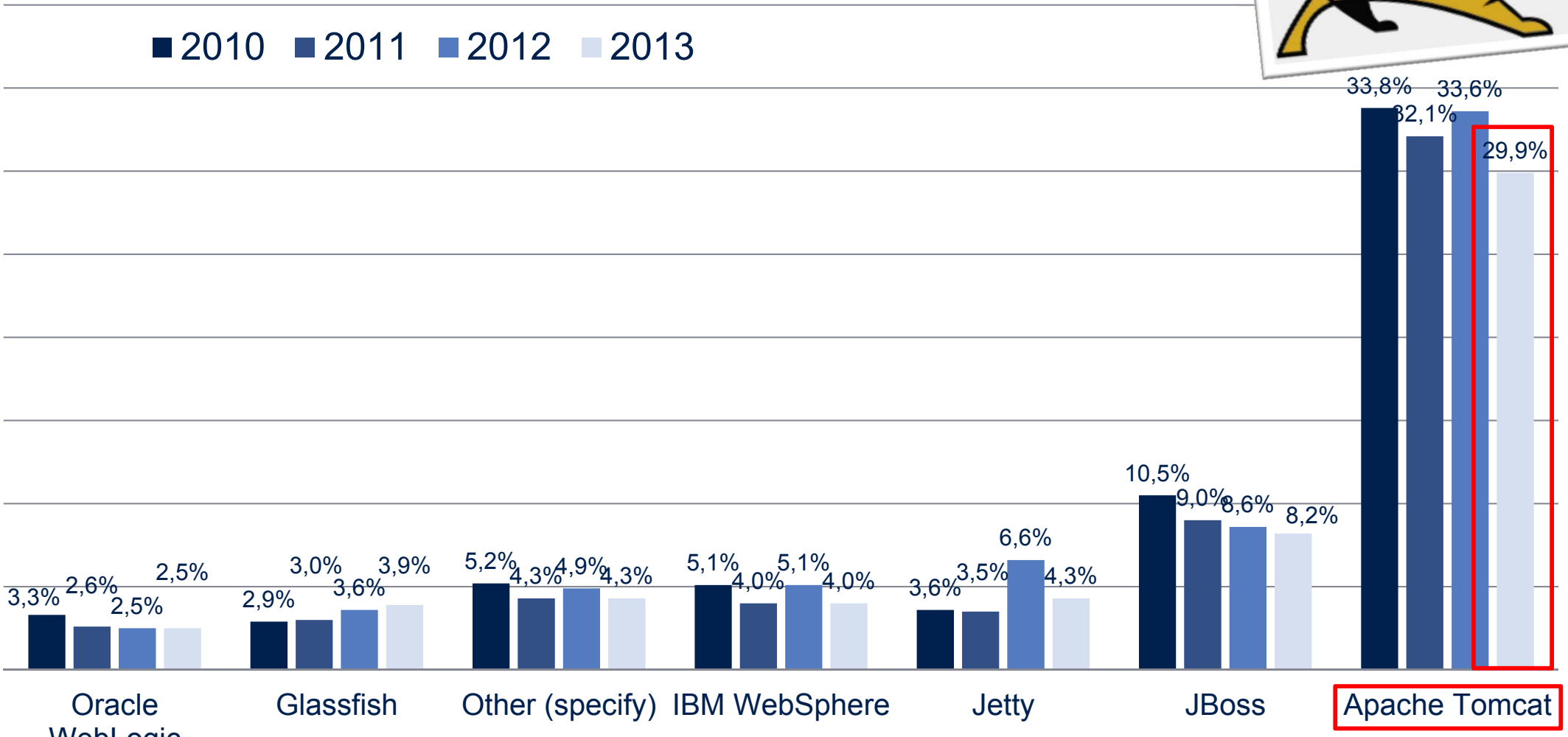
Robert Morris
Erster Wurm
*November 1988*



# Primary Application Server

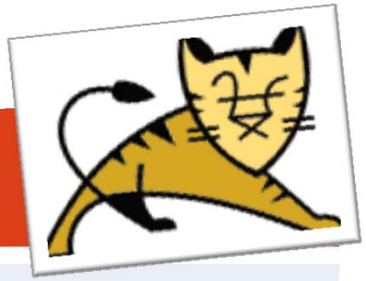


## What is the primary application server you typically use to deploy



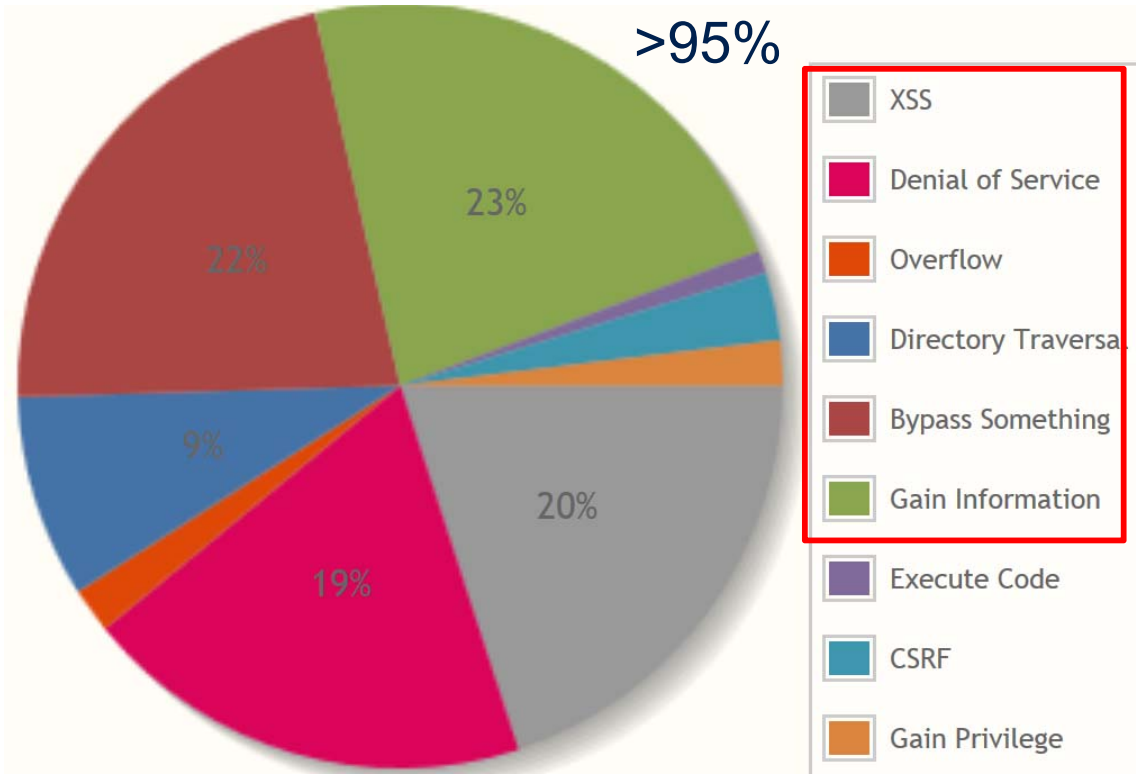

*Eclipse Open Source Developer Report 2013*

# Apache Tomcat Versionen



| Veröffentlicht | Servlet/ JSP Spec | | Tomcat Version | JDK, EL Version |
|---|---|---|---|---|
| **2013** | **3.1** | **2.3** | **8.0.x (8.0.7Beta)** | **JDK 1.7+(8), EL 3.0, TLS 1.2, JDBC 4.1** |
| 2010 | 3.0 | 2.2 | 7.0.x **(7.0.53/54)** | JDK 1.6+**(8)**, EL 2.2, TLS 1.0, JDBC 4.0 |
| 2006 | 2.5 | 2.1 | 6.0.x **(6.0.39/40)** | JDK 1.5+, 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 |
| *2001* | *2.3* | *1.2* | *4.1.40 (EOL)* | *JDK 1.3+, EL 1.0*, TLS 1.0 SunJSSE |
| *1999* | *2.2* | *1.1* | *3.3.2 (EOL)* | *JDK 1.2+*, TLS 1.0 SunJSSE Provider |

# Welche Tomcat-Schwachstellen? (cvedetails.com)




- [SECURITY] CVE-2012-3544 Chunked transfer encoding extension size is not limited
- [SECURITY] CVE-2013-2067 Session fixation with FORM authenticator
- [ANN] Apache Tomcat 7.0.40 released
- CVE-2013-2071 Request mix-up if AsyncListener method throws RuntimeException
- [ANN] Apache Tomcat 6.0.37 released
- [ANN] Apache Tomcat 7.0.39 released
- [ANN] Apache Tomcat 7.0.37 released
- [ANN] Apache Tomcat Native 1.1.27 released
- [ANN] Apache Tomcat 7.0.35 released
- Re: [ANN] End of life for Apache Tomcat 5.5.x
- [ANN] Apache Tomcat 7.0.34 released
- CVE-2012-4431 Apache Tomcat Bypass of CSRF prevention filter
- CVE-2012-3546 Apache Tomcat Bypass of security constraints
- CVE-2012-4534 Apache Tomcat denial of service
- [ANN] Apache Tomcat 7.0.33 released
- Fwd: [ANN] Apache Tomcat 6.0.36 released
- [SECURITY] CVE-2012-3439 Apache Tomcat DIGEST authentication weaknesses
- [SECURITY] CVE-2012-2733 Apache Tomcat Denial of Service

CSRF-Bypass
DoS

Gain Information

DoS

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | CVE-2013-2067 | 287 | | 2013-06-01 | 2013-11-24 | 6.8 | None | Remote | Medium | Not required | Partial | Partial | Partial |

java/org/apache/catalina/authenticator/FormAuthenticator.java in the form authentication feature in Apache Tomcat 6.0.21 through 6.0.36 and 7.x before 7.0.33 does not properly handle the relationships between authentication requirements and sessions, which allows remote attackers to inject a request into a session by sending this request during completion of the login form, a variant of a session fixation attack.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | CVE-2012-4534 | 399 | DoS | 2012-12-19 | 2013-06-04 | 2.6 | None | Remote | High | Not required | None | None | Partial |

org/apache/tomcat/util/net/NioEndpoint.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28, when the NIO connector is used in conjunction with sendfile and HTTPS, allows remote attackers to cause a denial of service (infinite loop) by terminating the connection during the reading of a response.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | CVE-2012-4431 | 264 | Bypass CSRF | 2012-12-19 | 2013-10-30 | 4.3 | None | Remote | Medium | Not required | None | Partial | None |

org/apache/catalina/filters/CsrfPreventionFilter.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.32 allows remote attackers to bypass the cross-site request forgery (CSRF) protection mechanism via a request that lacks a session identifier.

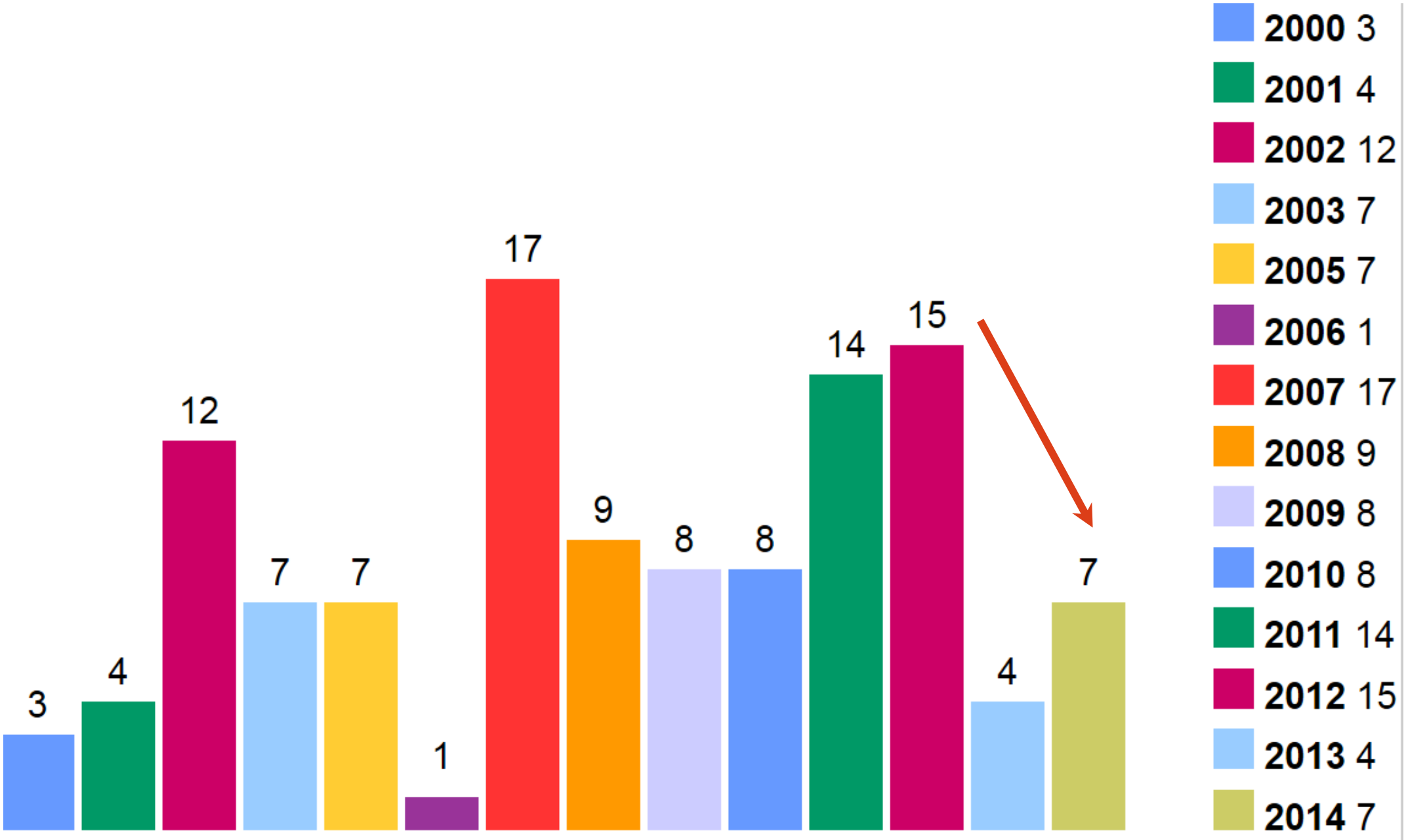
| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | CVE-2012-3546 | 264 | Bypass | 2012-12-19 | 2013-06-04 | 4.3 | None | Remote | Medium | Not required | None | Partial | None |

org/apache/catalina/realm/RealmBase.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.30, when FORM authentication is used, allows remote attackers to bypass security-constraint checks by leveraging a previous setUserPrincipal call and then placing /j_security_check at the end of a URI.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | CVE-2012-3544 | 20 | DoS | 2013-06-01 | 2013-06-14 | 5.0 | None | Remote | Low | Not required | None | None | Partial |

Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle chunk extensions in chunked transfer coding, which allows remote attackers to cause a denial of service by streaming data.

# Entwicklung der Tomcat-Schwachstellen? (cvedetails.com)



# Tomcat Sicherheit

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

[SECURITY] CVE-2013-4590 Information disclosure via XXE when running untrusted web applications
[SECURITY] CVE-2013-4322 Incomplete fix for CVE-2012-3544 (Denial of Service)
[SECURITY] CVE-2013-4286 Incomplete fix for CVE-2005-2090 (Information disclosure)
[SECURITY] CVE-2014-0033 Session fixation still possible with disableURLRewriting enabled
[ANN] Apache Tomcat 7.0.52 released
[SECURITY] CVE-2014-0050 Apache Commons FileUpload and Apache Tomcat DoS
[ANN] Apache Tomcat 8.0.1 (beta) available
[ANN] Apache Tomcat 6.0.39 released
[SECURITY] CVE-2012-3544 Chunked transfer encoding extension size is not limited
[SECURITY] CVE-2013-2067 Session fixation with FORM authenticator
[SECURITY] CVE-2012-3439 Apache Tomcat DIGEST authentication weaknesses
[SECURITY] CVE-2012-2733 Apache Tomcat Denial of Service

**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 |
| Total   26 bugs                                                         |
+-------------------------------------------------------------------------+
```

**JDK**
Key: JDK | Lead: J. Duke | Category: Open JDK Projects

Summary
Issues
Road Map
Change Log
Popular Issues
Versions

**Change Log**

A list of released versions. Click on the row to display issues for that version.
previous 10 versions | **all versions**

| | | |
|---|---|---|
| 7u51 | Release Date: **2014-01-13** Release Notes | CPU14_01 |
| 7u45 | Release Date: **2013-10-14** Release Notes | CPU13_04 |

| | |
|---|---|
| 7u75 | Release Date: 2015-01-19 |
| 8u31 | Release Date: 2015-01-19 |
| 5.0u75 | Release Date: 2014-10-13 |
| 6u85 | Release Date: 2014-10-13 |
| 7u71 | Release Date: 2014-10-13 |
| 8u25 | Release Date: 2014-10-13 |

**Fixed in Apache Tomcat 7.0.33** **released 21 Nov 2012**

**Important: Session fixation** CVE-2013-2067

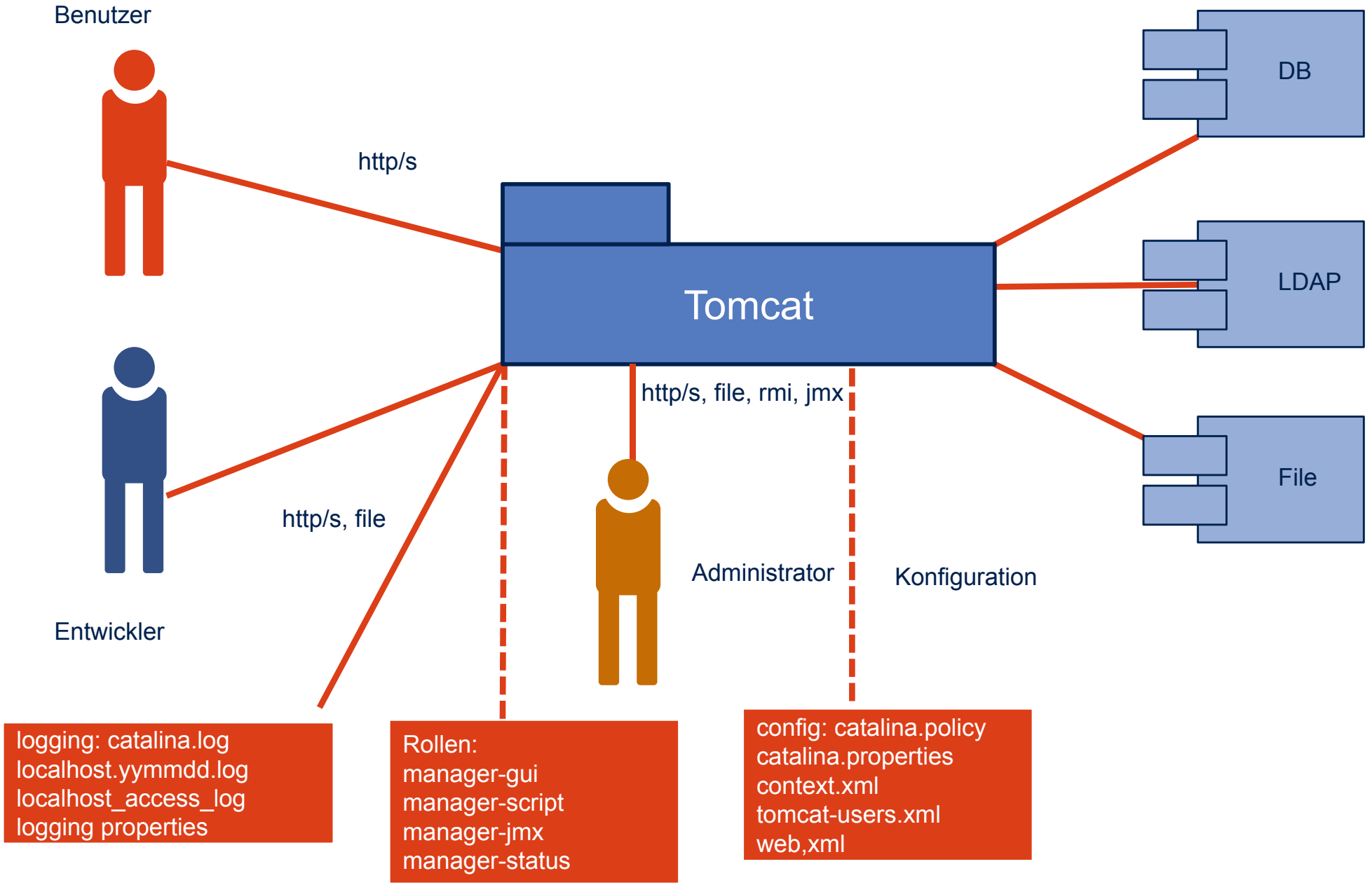
FORM authentication associates the most recent request requiring authentication with the current session. By repeatedly sending a request for an authenticated resource while the victim is completing the login form, an attacker could inject a request that would be executed using the victim's credentials.

This was fixed in revision 1408044.

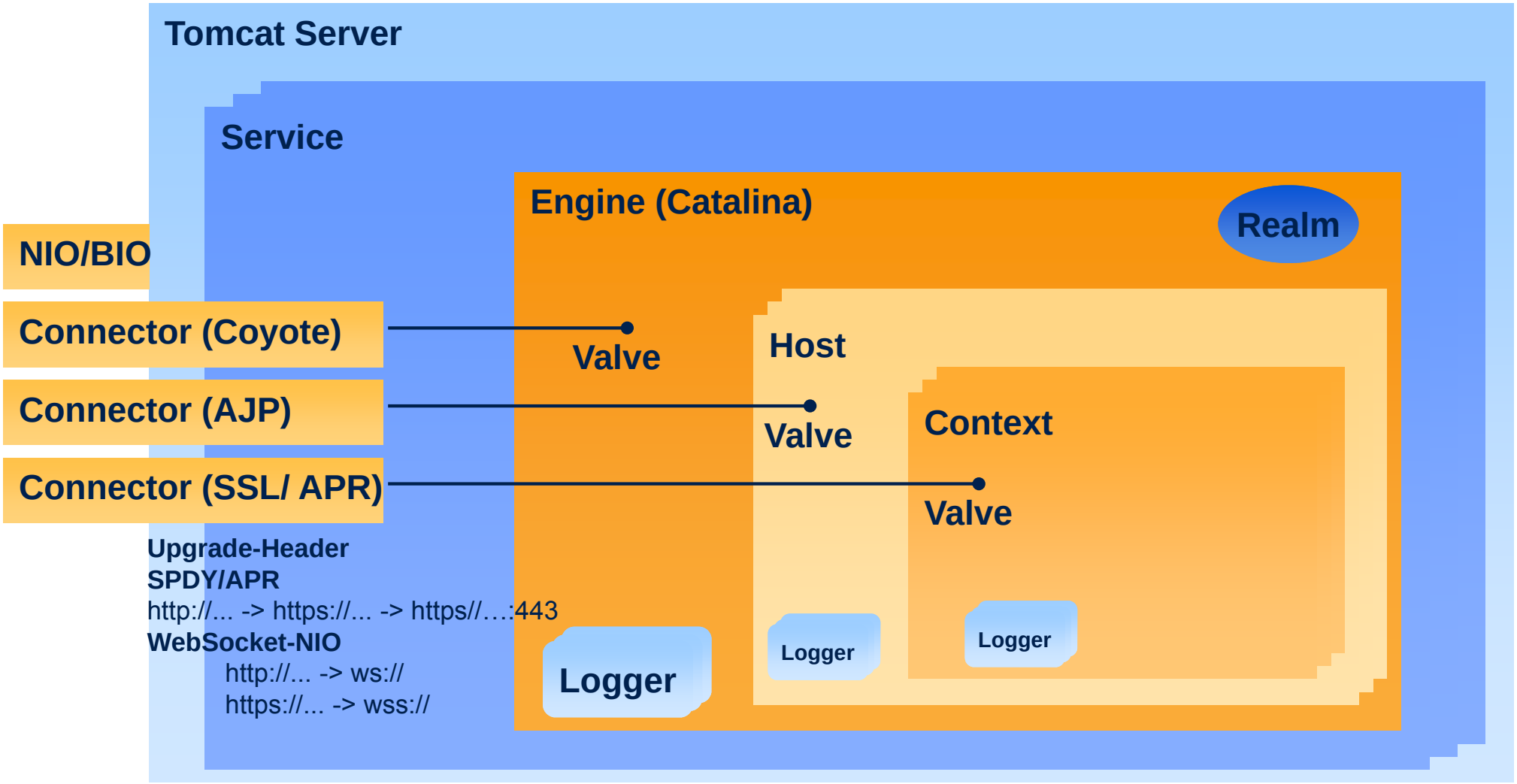
This issue was identified by the Tomcat security team on 15 Oct 2012 and made public on 10 May 2013.

Affects: 7.0.0-7.0.32

# Tomcat-Überblick: Sicherheits-Kontext

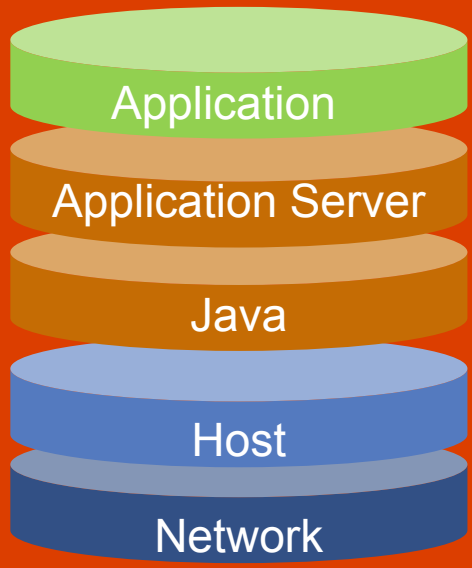


# Architektur - Tomcat Komponenten



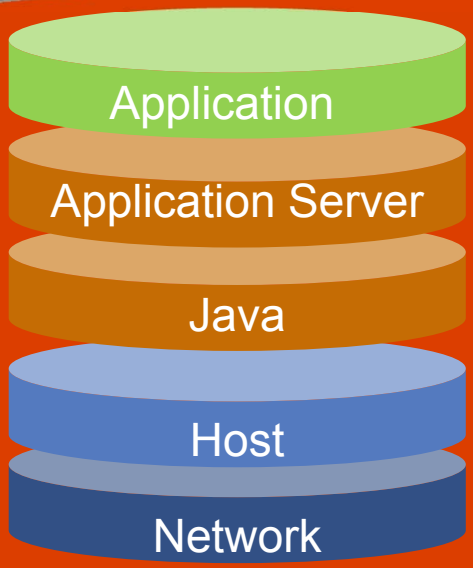
# Sicherheit aber wie?

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



# Wie überwachen? Wie managen?

- access_log → auswerten Auffälligkeiten, Fehlercodes
- JMX → Ressourcen-Verbrauch
- Manager → Konfiguration, Ressourcen, Anwendungen
- CVEchecker, CVE Dependency-Check

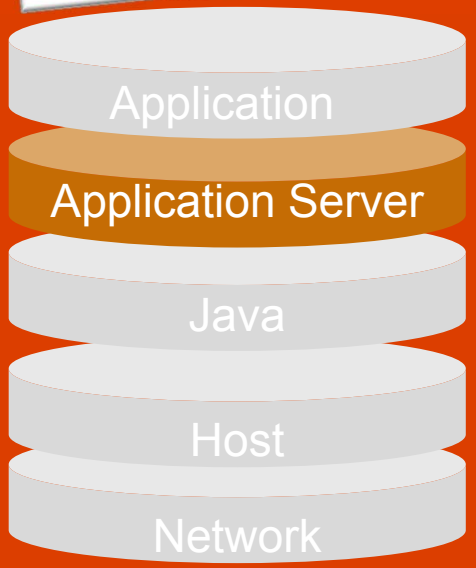


# Sicherheit von Anfang an - abspecken

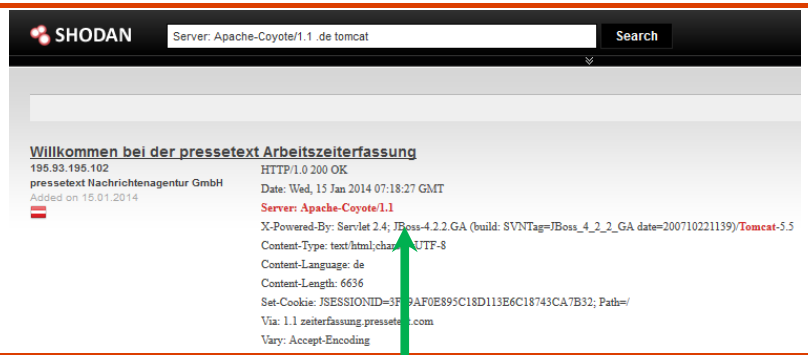
- Installationsdatei verifizieren

```
md5sum -c apache-tomcat-8.0.3.zip.md5
```

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



# Tarnen, täuschen, Produktversion verschleiern




*cd CATALINA_HOME/lib*

*jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties*

*ServerInfo.properties server.info=Apache*
*server.number=0.0.0.0*

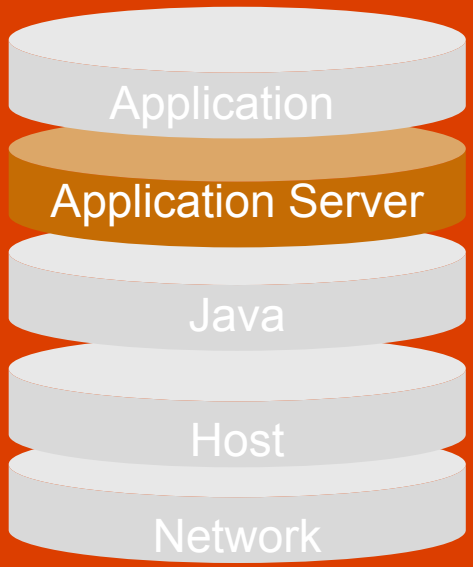
*jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties*

*CATALINA_HOME/conf/server.xml*

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

Testen: version.[sh|bat]

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



# Authentifizierung & Authorisierung für Webanwendungen

Zugriffsmethoden:

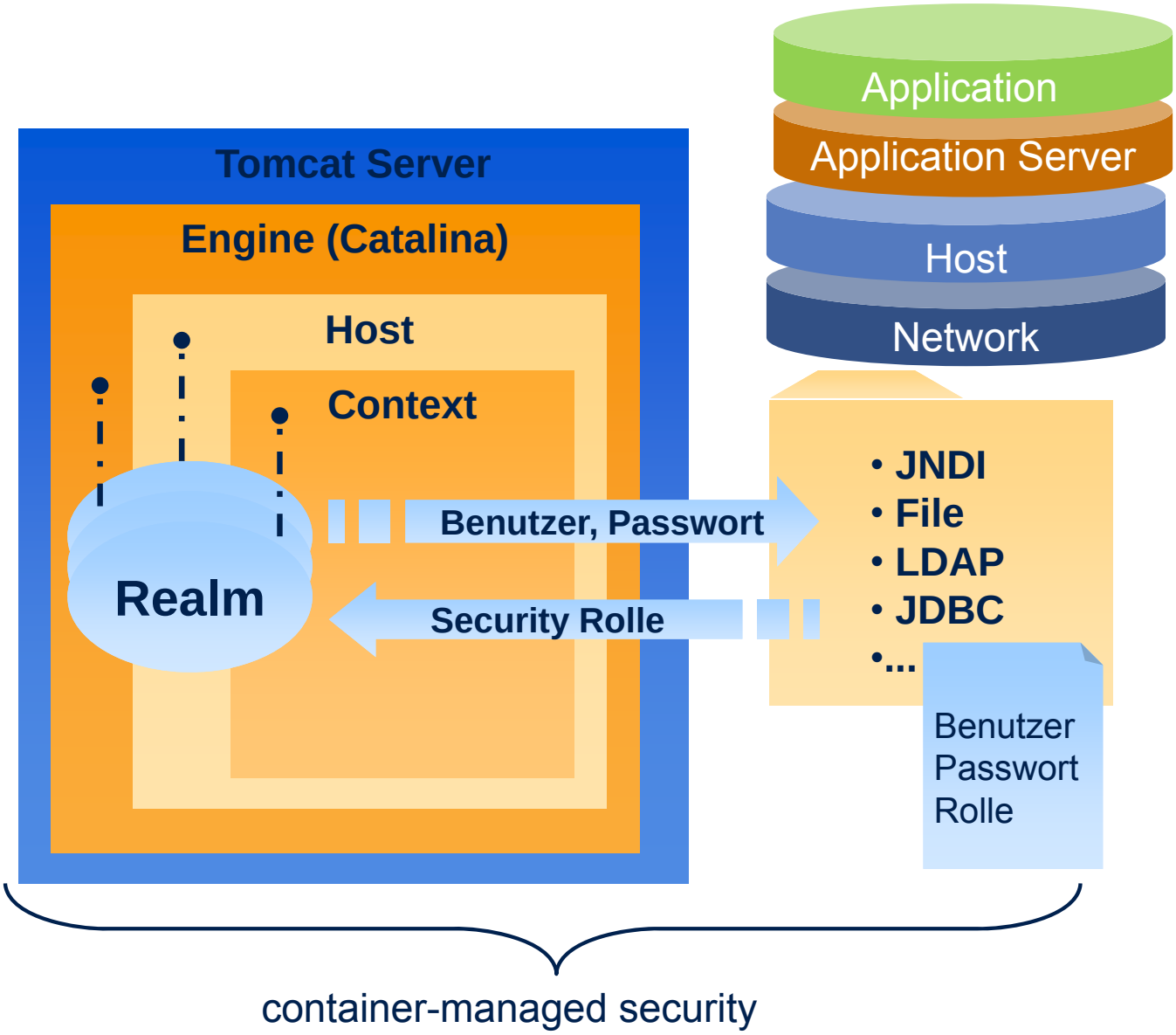
**BASIC (RFC-2617)**

**FORM based (RFC-2617)**

**DIGEST**

**CLIENT-CERT**

- Create: • HTTP PUT
- Read: • HTTP GET
- Update: • HTTP POST
- Delete: • HTTP DELETE



# 2013-A2 Broken Authentication: Verschlüsselte Passwörter gestern & heute

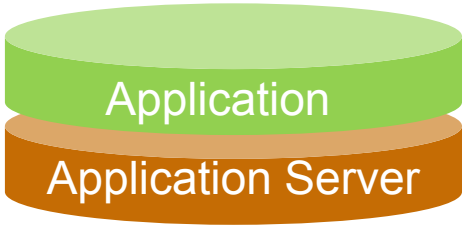
# OWASP Top 10 für Entwickler-2013: A8 Cross-Site Request Forgery

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

| Bedrohungs-quelle | Angriffs-vektor | Schwachstellen | | Technische Auswirkung | Auswirkung auf das Unternehmen |
|---|---|---|---|---|---|
| ——— | Ausnutzbarkeit<br>DURCHSCHNITTLICH | Verbreitung<br>HÄUFIG | Auffindbarkeit<br>EINFACH | Auswirkung<br>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.<br>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.<br>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

# 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>
configured webserver -->
</cookie-config>
        <tracking-mode>COOKIE</tracking-mode>
    </session-config>
</web-app>
```


**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**

# Cross Site Request Forgery Protection with Token in Java-Servlets/JSF


- **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

# 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


A9 - Using Components with Known Vulnerabilities

# Security by obscurity: Manager Webanwendung umbenennen oder entfernen

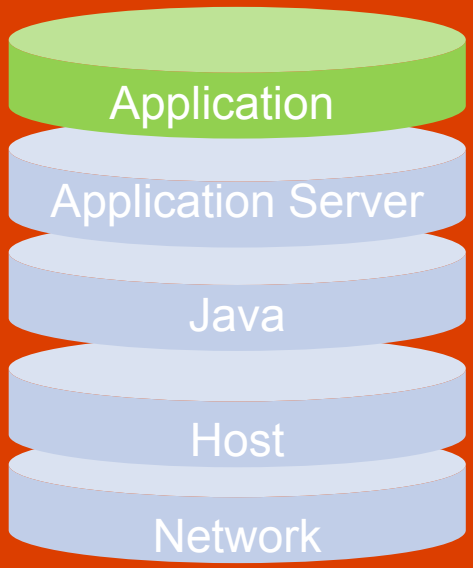
mv **CATALINA_HOME**/conf/Catalina/localhost/**manager.xml** **CATALINA_HOME**/conf/Catalina/localhost/**foobar.xml**

vi **CATALINA_HOME**/conf/Catalina/localhost/**foobar.xml**
${catalina.home}/server/webapps/foobar

mv **CATALINA_HOME**/server/webapps/**manager** **CATALINA_HOME**/server/webapps/**foobar**

vi **CATALINA_HOME**/conf/Catalina/**tomcat-users.xml**

```
<role rolename="manager"/> <user username=„chef" password="ReallyComplexPassword" roles="manager"/>
```

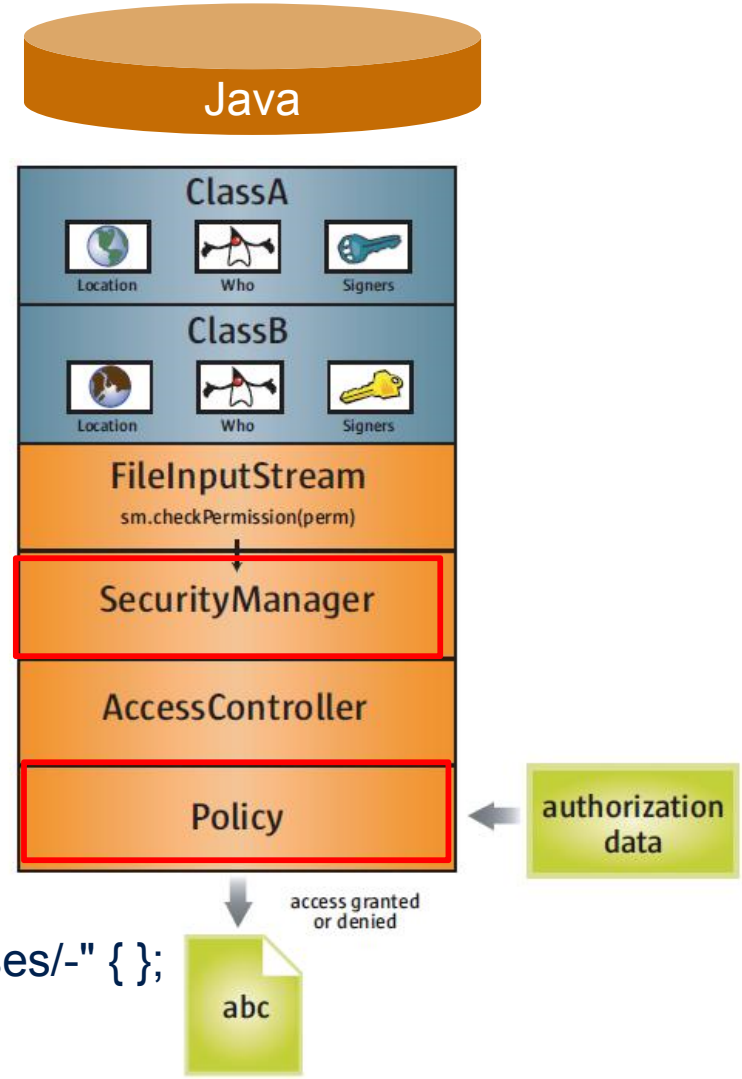


# Java-Policies anwenden

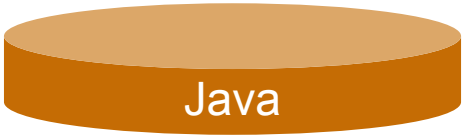
## conf

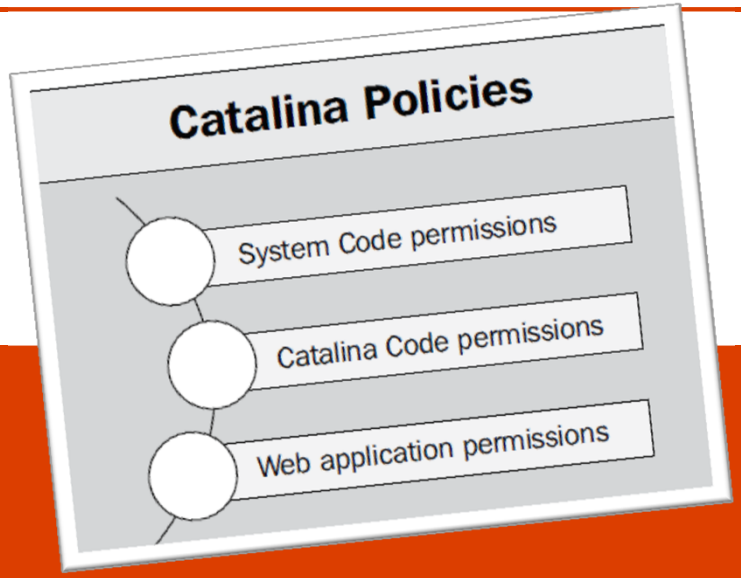
- catalina.properties
- catalina.policy

```
// These permissions apply to javac
grant codeBase "file:${java.home}/lib/-" {
        permission java.security.AllPermission;};
// These permissions apply to the servlet API classes
// and those that are shared across all class loaders
// located in the "lib" directory
grant codeBase "file:${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

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.

BSI

secorvo

**Zertifizierungs-infrastruktur für die PKI-1-Verwaltung**

**Umsetzungskonzept für die Anwendung von SSL**

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

Version 1.4
Stand 10.12.2002

**Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen**

**Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung**

**(Übersicht über geeignete Algorithmen)**

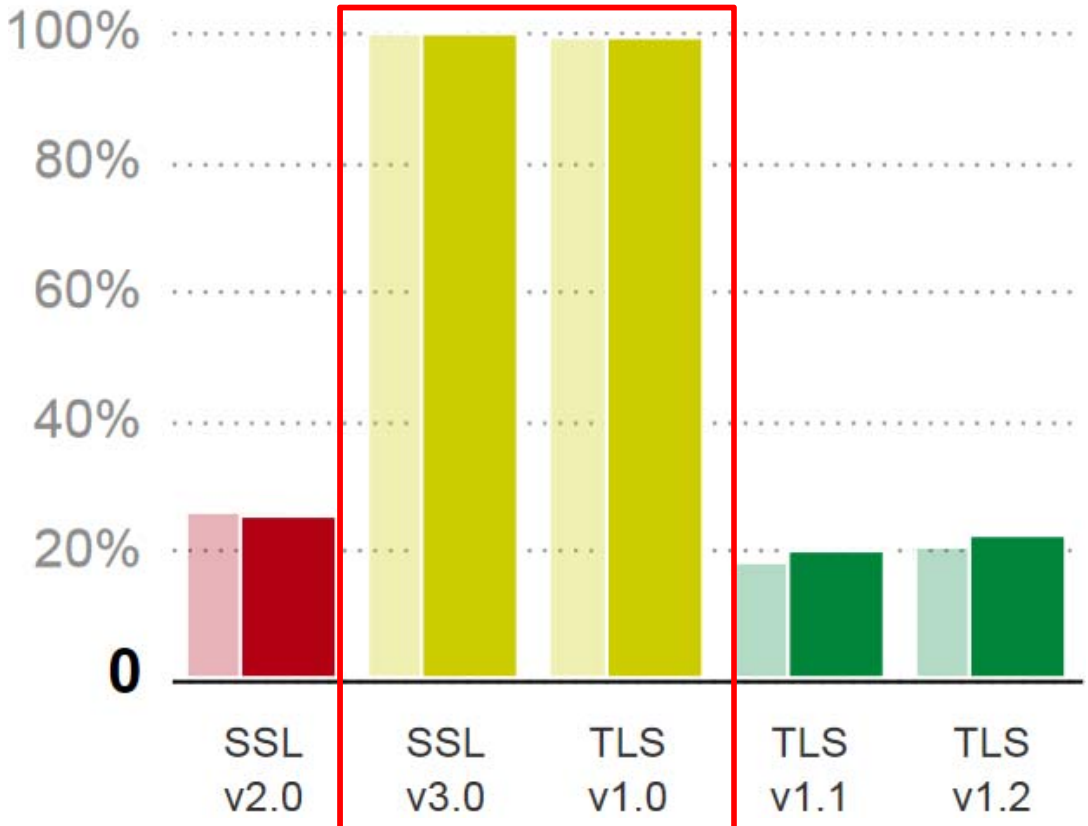
**Vom 13. 1. 2014**

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde gemäß § 3 Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), veröffentlicht gemäß Anlage 1 Abschnitt 1 Nr. 2 Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542), im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt.

**Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001**

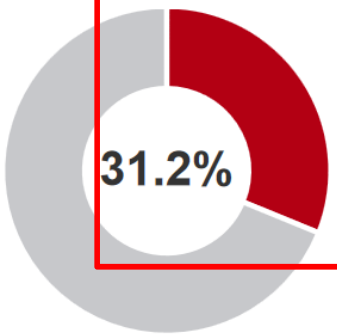
# https://www.trustworthyinternet.org/ssl-pulse/

## Protocol Support




**31.2** % of sites surveyed support ciphers weaker than **128** bits

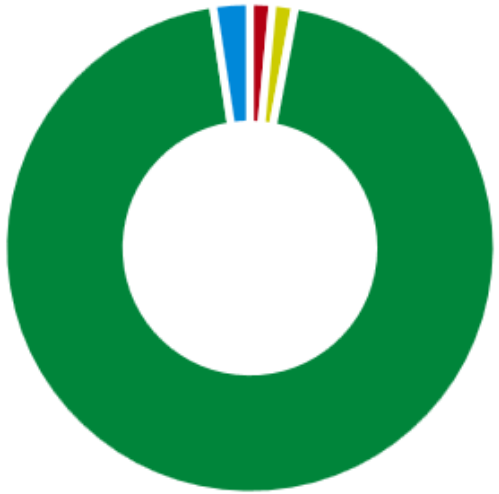
**50,310 sites**




Sites that support weak or insecure cipher suites

**50,310**

**- 0.4 %**

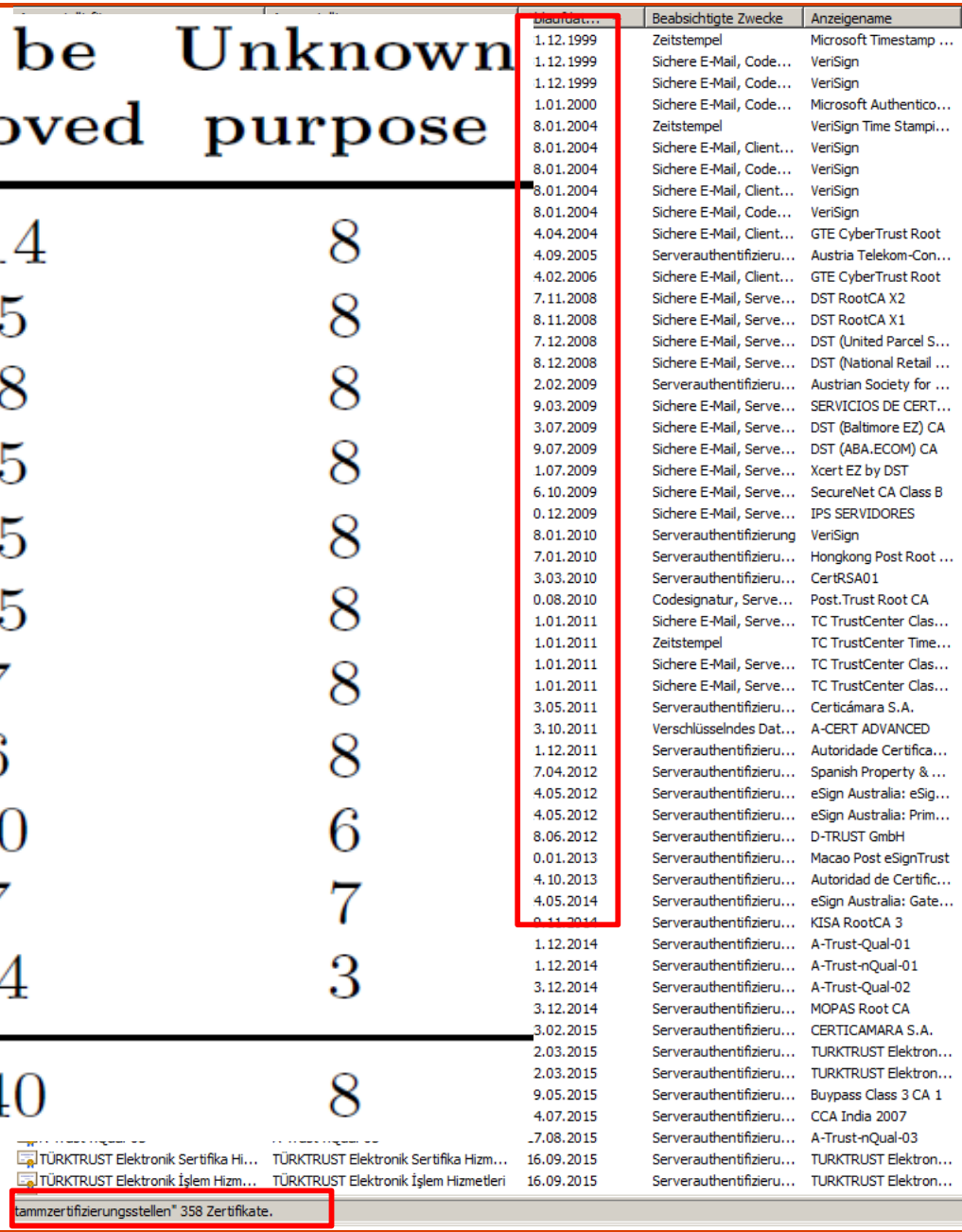


## Key Strength Distribution

- Below 1024 bits
  **29** < 0.1%
  **+ 0.0 %**
- 1024 bits
  **2,122** 1.3%
  **- 0.4 %**
- 2048 bits
  **155,204** 96.2%
  **+ 0.3 %**
- 4096 bits
  **3,947** 2.4%
  **+ 0.0 %**

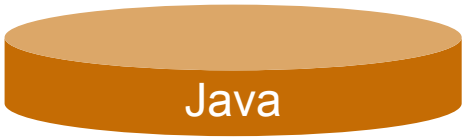
# Unbenutzte, abgelaufene Zertifikate entfernen (Prel, Fahl, Smith, Uni Bonn, Hannover 2014)

| Platform | Total certs | Unused certs | To be removed | Unknown purpose |
|---|---|---|---|---|
| Windows | 377 | 122 | 114 | 8 |
| Mozilla | 172 | 23 | 15 | 8 |
| OS X/iOS | 207 | 46 | 38 | 8 |
| Ubuntu | 159 | 23 | 15 | 8 |
| Debian | 159 | 23 | 15 | 8 |
| Gentoo | 159 | 23 | 15 | 8 |
| Android | 146 | 15 | 7 | 8 |
| openSUSE | 144 | 14 | 6 | 8 |
| CentOS | 120 | 16 | 10 | 6 |
| BlackBerry | 90 | 14 | 7 | 7 |
| OpenBSD | 60 | 17 | 14 | 3 |
| total | 431 | 148 | 140 | 8 |




Java-JRE-Keystore enthält 78 Einträge

# 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*) -Djava.security.egd=file:/dev/urandom*

# 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)<br>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

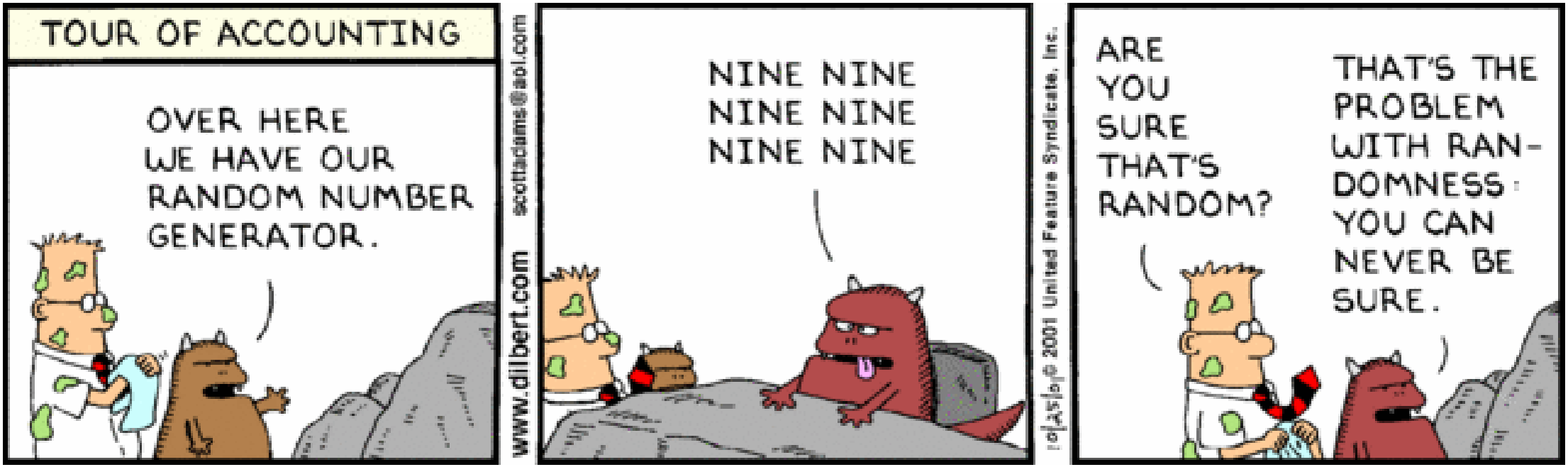
The algorithm name in this section can be specified when generating an instance of `SecureRandom`.

| 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

# Pseudozufallszahlengenerator (PNRG)

**Java**
Random seit 1.0
ThreadLocalRandom seit 1.7
SplittableRandom, new SecureRandom(seed).getInstanceStrong() seit 1.8
Guter Entropie-Pool wichtig!!!

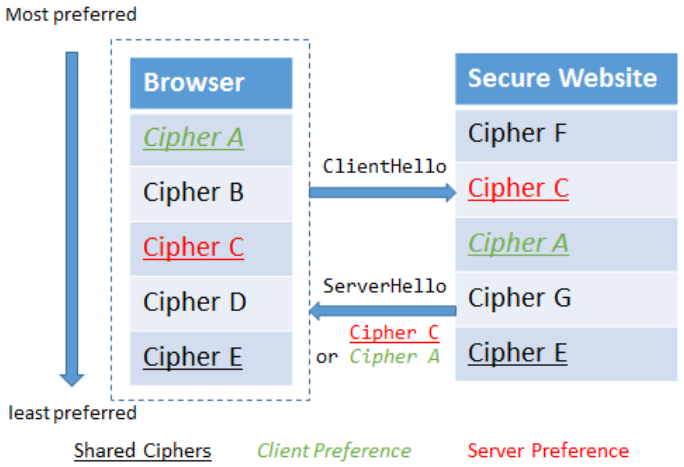


# Welche Chiffren?


*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

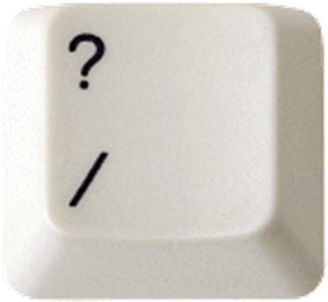

Kontrolle: http://localhost:8080/manager/text/sslConnectorCiphers

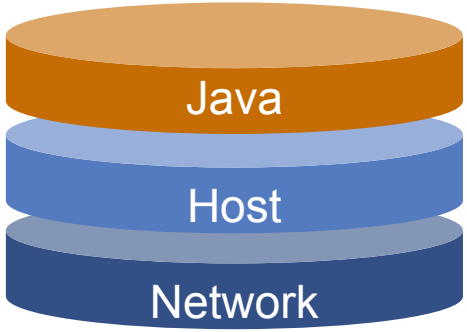
**server.xml**

<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="SSL_RSA_WITH_RC4_128_MD5, **SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA**, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA" keystoreFile="mydomain.key" keystorePass="password" truststoreFile="mytruststore.truststore" truststorePass="password"/>

<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" />

# Secure Sockets Layer (SSL) mit Tomcat




**Zwei Konnektoren:**

- JSSE protocol="org.apache.coyote.http11.**Http11NioProtocol**“ (TLS 1.x)
- APR's OpenSSL 1.0.1e Tomcat Native 1.1.24 - 1.1.29 Bug 56363 -> **1.1.30** protocol="org.apache.coyote.http11.**Http11AprProtocol**“ (nur **TLS 1.0**, dafür schneller und weitere Chriffrensammlungen Bug 53952 support TLS 1.1 & 1.2 )

**Keystore-Formate:**

- **JKS** (Java KeyStore): java **keytool** Werkzeug
- **PKCS12** (Public Key Cryptography Personal Information Exchange Syntax Standard der RSA Security Organisation): Werkzeug **OpenSSL**

# https://www.ssllabs.com/ssltest/analyze.html

## SSL Report: entwicklertag.de (80.86.165.174)

Assessed on: Wed Mar 12 14:57:22 UTC 2014 | Clear cache

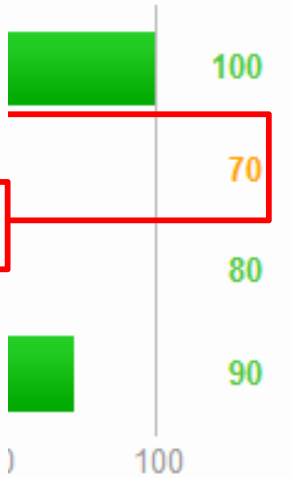
Sc

### Protocols

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

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

| | |
|---|---|
| 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_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 128 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | 112 |
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits (p: 128, g: 1, Ys: 128) FS | 112 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | 256 |




SSL Cookbook.

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

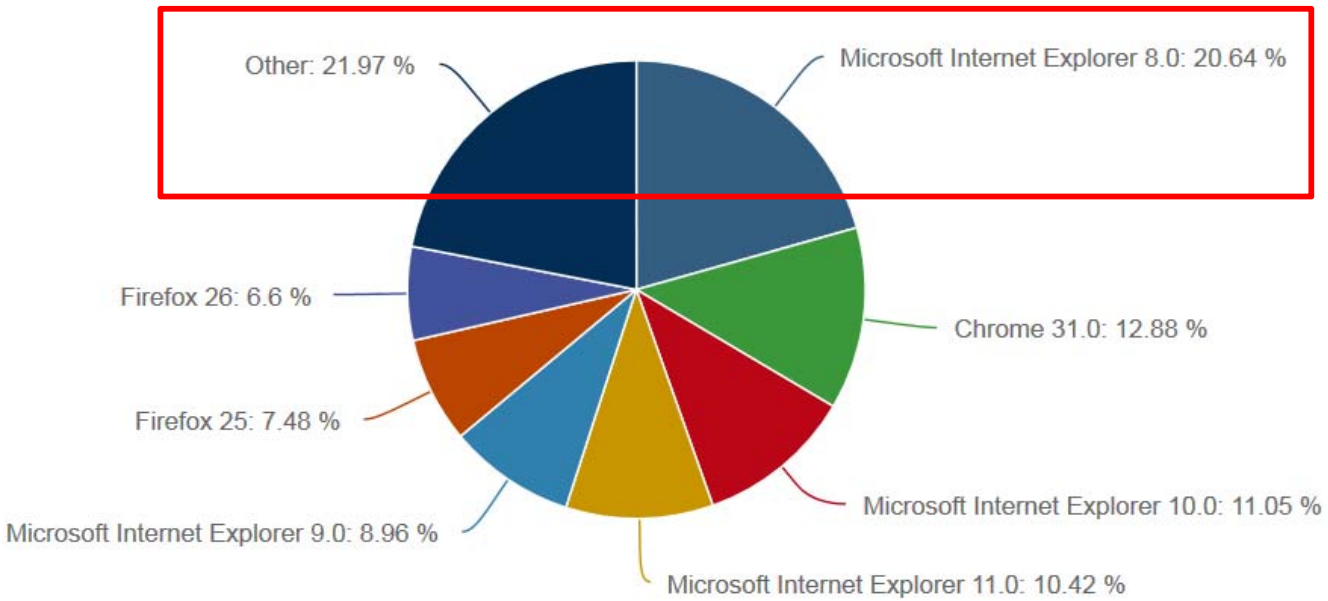
# http://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers

| Browser | Version | Platforms | TLS 1.0 | TLS 1.1 | TLS 1.2 |
|---|---|---|---|---|---|
| Chrome [notes 2] [notes 3] | 0–21 | Android, iOS, Linux, Mac OS X, Windows (XP, Vista, 7, 8) | Yes | No | No |
| | 22–29 | | Yes [32] | Yes | No [32][33][34][35] |
| | 30– | | Yes [32] | Yes [32] | Yes [33][34][35] |
| Firefox [notes 3] [notes 4] | 1–18 ESR 10, 17 | Android, Linux, Mac OS X, Windows (XP, Vista, 7, 8) | Yes [36] | No [28] | No [30] |
| | 19–23 | | Yes [36] | Yes, disabled by default [28][37] | No[30] |
| | 24–26 ESR 24 | | Yes [36] | Yes, disabled by default [28][37] | Yes, disabled by default [30][38] |
| | 27– ESR 31– | | Yes [36] | Yes [28][37][39] | Yes [30][38][39] |
| 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 [42] | Yes [42] |

# 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)



# 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 |

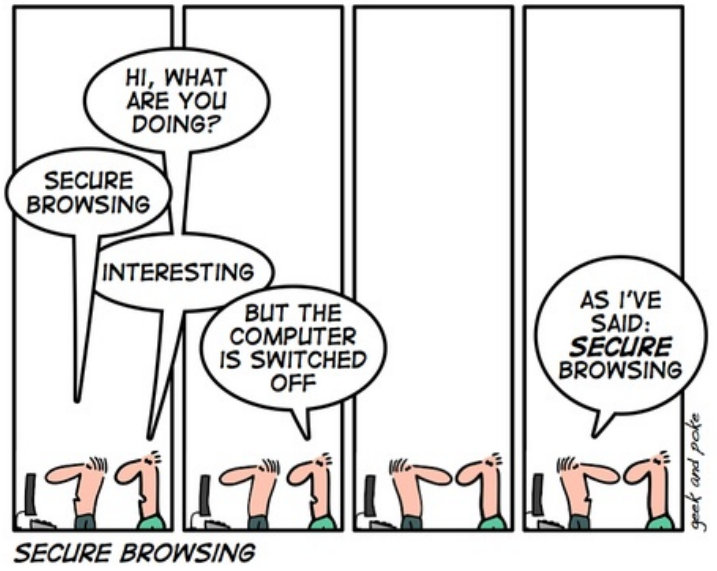
(*) This test reliably detects only the highest supported protocol.

**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

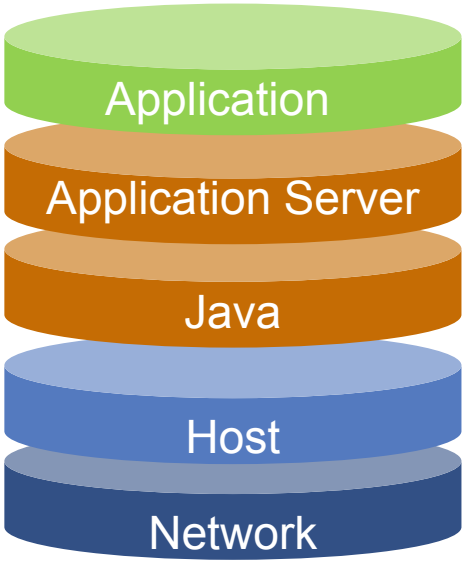
# Fazit: Apache Tomcat aber sicher!

- 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?

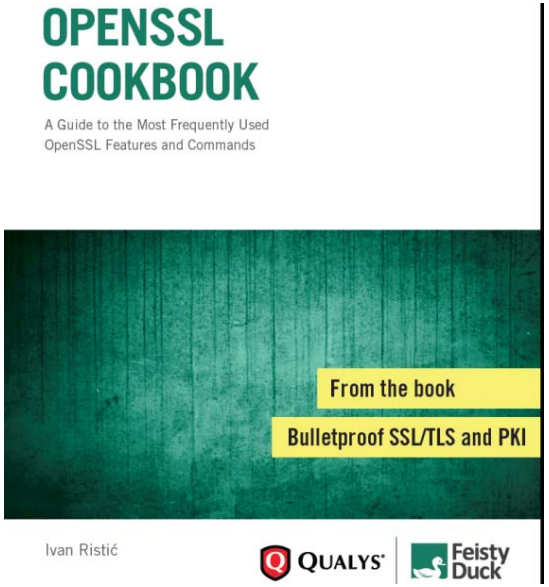
# Ausblick – Kryptokalypse?

- **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!

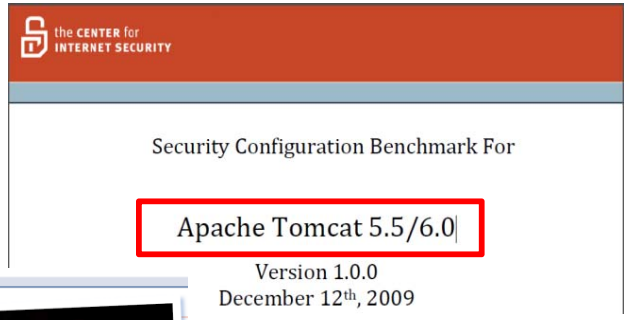



# Weitere Infos

- 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
- 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









# Vielen Dank für Eure Aufmerksamkeit!


**MATERNA GmbH**
**Dipl. Inform. Frank Pientka**
Software Architect
Business Division Applications

Telefon: +49 231 5599-8854
Telefax: +49 231 5599-272
E-Mail: Frank.Pientka@materna.de