NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

**CỤC CÔNG NGHỆ THÔNG TIN**



**PHỤ LỤC 01**

**TÀI LIỆU HƯỚNG DẪN NÂNG CẤP CHƯƠNG TRÌNH CITAD**

**PHIÊN BẢN 5.0.0.2.0.0**

*(kèm theo Công văn số ……/CNTT5 ngày …./…../2020 về việc Ban hành phiên bản CITAD 5.0.0.2.0.0)*

**Hà Nội, Tháng 06 năm 2020**

**MỤC LỤC**

[**A. Mục tiêu tài liệu 3**](#_Toc42855281)

[**B. Nội dung tài liệu 6**](#_Toc42855282)

[I. Chuẩn bị trước khi nâng cấp 6](#_Toc42855283)

[I.1. Backup hệ thống CITAD phiên bản đang sử dụng 6](#_Toc42855284)

[I.1.1. Backup ứng dụng 6](#_Toc42855285)

[a. Backup chương trình CITAD\_WEB 6](#_Toc42855286)

[b. Backup chương trình IBPSCommunication 6](#_Toc42855287)

[I.1.2. Backup Database 6](#_Toc42855288)

[a. Backup Database phiên bản Oracle 6](#_Toc42855289)

[b. Backup Database phiên bản SQL Server 6](#_Toc42855290)

[II. Thực hiện nâng cấp phiên bản 6](#_Toc42855291)

[II.1. Nâng cấp phiên bản TAD\_COMM 7](#_Toc42855292)

[II.2. Nâng cấp phiên bản TAD\_WEB 7](#_Toc42855293)

[II.3. Nâng cấp phiên bản CITAD Client 7](#_Toc42855294)

[III. Hướng dẫn phục hồi phiên bản cũ đang sử dụng 8](#_Toc42855295)

[III.1. Phục hồi ứng dụng 8](#_Toc42855296)

[III.1.1. Phục hồi chương trình CITAD\_WEB 8](#_Toc42855297)

[III.1.2. Phục hồi chương trình IBPSCommunication 8](#_Toc42855298)

[III.2. Phục hồi Database 8](#_Toc42855299)

[IV. Khuyến cáo về an ninh bảo mật 9](#_Toc42855300)

[IV.1. Khuyến cáo xóa các file .jar của Tuxedo 9](#_Toc42855301)

**Tài liệu hướng dẫn nâng cấp chương trình**

**CITAD phiên bản 5.0.0.2.0.0**

1. Mục tiêu tài liệu

Tài liệu này nhằm hướng dẫn các đơn vị thành viên (CI) thực hiện nâng cấp chương trình CITAD lên phiên bản 5.0.0.2.0.0.

**Bảng danh sách các chức năng được nâng cấp trong phiên bản:**

| **STT** | **Nội dung nâng cấp** | **Mô tả** |
| --- | --- | --- |
| **I** | **TAD\_COMM** | |
|  | Cập nhật CI-Gateway | Sửa một số lỗi import, export giao dịch qua ci-gateway |
|  | Tăng tốc độ giải nén dữ liệu file đến | Thực hiện tăng tốc độ giải nén dữ liệu file đến |
|  | Bổ sung ghi log ứng dụng | Ghi thêm log 1 số thao tác: đăng nhập, đăng xuất, thay đổi cấu hình hệ thống |
|  | Cập nhật chức năng yêu cầu nhận file từ TTXL | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng yêu cầu nhận file ở TAD\_COMM (II.2.4.4,II.2.4.5,II.2.4.6) |
|  | Hiển thị tình trạng file đang xử lý | Giao diện TAD\_COMM, menu nhận dữ liệu, hiển thị tình trạng file đang xử lý |
|  | Bổ sung liên quan đến giao dịch quyết toán lô | Cập nhật dữ liệu quyết toán lô đến |
| **II** | **TAD\_WEB** | |
|  | Tự động làm mới trang dashboard | Trang Dashboard tại TAD\_WEB, sau 1 phút tự động làm mới. |
|  | Đồng bộ bảng danh sách dịch vụ ngoại tệ của các Ngân hàng từ NPSC xuống CI | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng bảng mã ngân hàng (II.1.2.3.1.1) |
|  | Fix lỗi In giấy báo bị chèn đè thông tin giữa các trường dữ liệu có nội dung dài trên khổ giấy A5 | TAD\_WEB cho phép in giấy báo ra khổ A4, Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng in giấy báo (II.1.2.4.3.4) |
|  | Sửa lỗi in lũy kế | Bổ sung dữ liệu thu NSNN |
|  | Đối với giao dịch thu NSNN: Bỏ ràng buộc bắt buộc đối với Tên người nhận=Tên cơ quan thu và cho phép nhập Tên người nhận như giao dịch bình thường. | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng tạo lệnh chuyển tiền (II.1.2.4.2.1.a.1) |
|  | Cho phép thoái/ trả lại giao dịch theo lô: nội dung thoái/trả lại của mỗi bút toán lấy theo bút toán đầu tiên.  Khi thực hiện thoái, trả lại bút toán trong màn hình chi tiết: nội dung trả lại của mỗi bút toán phải nhập mới. | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng kiểm soát lệnh chuyển tiền (II.1.2.4.2.1.a.3) |
| **III** | **Giao dịch quyết toán lô** | |
|  | Màn hình Dashboard bổ sung thống kê yêu cầu quyết toán lô đến | Màn hình Dashboard bổ sung thống kê yêu cầu quyết toán lô đến |
|  | Tra cứu dữ liệu yêu cầu quyết toán lô đến | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng tra cứu dữ liệu (II.1.2.4.2.6.c) |
|  | Theo dõi Ci-Gateway trả lời tra soát, quyết toán lô | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng theo dõi giao dịch xử lý qua CI\_GATEWAY (II.1.2.4.2.5.g, II.1.2.4.2.6.e) |
|  | Cho phép in giấy báo quyết toán lô đến | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng kiểm soát yêu cầu quyết toán lô đến (II.1.2.4.2.6.b) |
|  | Thông báo tới Đơn vị thành viên thiếu số dư trong lô quyết toán. | Tham khảo tài liệu hướng dẫn sử dụng CITAD, chức năng (II.1.2.4.2.6.a) |
| **IV** | **Nâng cấp khác** | |
|  | ANBM | Đáp ứng các yêu cầu ANBM đã được khuyến cáo. |

*Mọi thắc mắc trong quá trình nâng cấp đề nghị liên hệ bộ phận hỗ trợ của Cục Công nghệ thông tin, điện thoại: 024 32595986, email:* [*hotrotinhoc@sbv.gov.vn*](mailto:hotrotinhoc@sbv.gov.vn) *hoặc theo danh sách dưới đây để được giải đáp.*

**Đầu mối hỗ trợ nâng cấp CITAD phiên bản 5.0.0.2.0.0 :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TT | Tên | Email | SĐT | Ghi chú |
| 1 | Nguyễn Thái Phụ Dũng | [dung.nguyenthai@sbv.gov.vn](mailto:dung.nguyenthai@sbv.gov.vn) | 0946221230 | Chuyên viên Cục CNTT |
| 2 | Vũ Văn Cường | cuong-vv@hipt.vn | 0915163888 | Nhân viên công ty HIPT |
| 3 | Nguyễn Thị Phương Anh | [anh-np@hipt.vn](mailto:anh-np@hipt.vn) | 098 3373384 | Nhân viên công ty HIPT |
| 4 | Trương Thị Xen | xen-tt@hipt.vn | 0973681358 | Nhân viên công ty HIPT |
| 5 | Nguyễn Văn Trung | trung-nv@hipt.vn | 0984530369 | Nhân viên công ty HIPT |
| 6 | Nguyễn Đình Sơn | son-nd@hipt.vn | 0379142889 | Nhân viên công ty HIPT |

1. Nội dung tài liệu
   1. Chuẩn bị trước khi nâng cấp
      1. Backup hệ thống CITAD phiên bản đang sử dụng

***Chú ý*** : ***Đối với các Chi nhánh NHNN chỉ backup TAD\_COMM.***

* + - 1. Backup ứng dụng
         1. Backup chương trình CITAD\_WEB

Backup toàn bộ thư mục CITAD là thư mục cài đặt của chương trình sang ổ đĩa mới. Đường dẫn trên máy cài đặt ứng dụng CITAD có dạng như sau:

* Ổ đĩa:\inetpub\wwwroot\**CITAD**
  + - * 1. Backup chương trình IBPSCommunication

Backup toàn bộ thư mục IBPSCommunication là thư mục cài đặt của chương trình sang ổ đĩa hoặc máy mới. Đường dẫn trên máy cài đặt ứng dụng IBPSCommunication có dạng như sau:

* Ổ đĩa:\Program Files....\SBV\**IBPSCommunication**
  + - 1. Backup Database

Backup database là backup toàn bộ cấu trúc và dữ liệu của cơ sở dữ liệu CITAD, do cán bộ quản trị cơ sở dữ liệu của đơn vị chủ động thực hiện theo phương thức phù hợp với hạ tầng của đơn vị. Việc backup database phải đảm bảo khả năng khôi phục database CITAD về thời điểm ngay trước khi thực hiện nâng cấp. Khi thực hiện backup database có thể tham khảo một trong số các cách dưới đây.

* + - * 1. Backup Database phiên bản Oracle

Sử dụng công cụ expdp của Oracle để export Schema CITAD; Schema CIGATEWAY ra file .dmp. Sau khi export ra file .dmp thành công thì copy các file này sang ổ đĩa hoặc máy mới

* + - * 1. Backup Database phiên bản SQL Server

Sử dụng công cụ SQL Server Managerment Studio để stop SQL Server sau đó thực hiện copy backup sang ổ đĩa hoặc máy mới các file .mdf; .ldf của Database CITAD và Database CIGATEWAY

* 1. Thực hiện nâng cấp phiên bản

Link download phiên bản CITAD mới như sau:

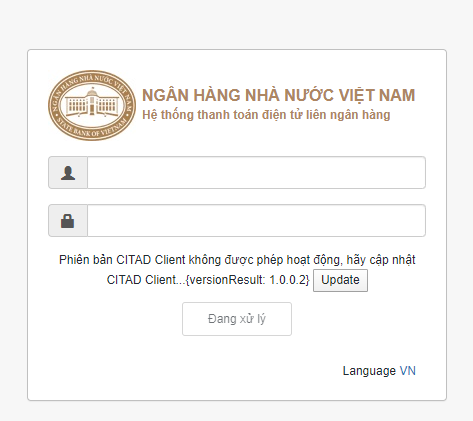
<https://drive.google.com/drive/folders/1wjwHj_2_j90dzRomYZCY4AfuEXLJSc4E?usp=sharing>

***Chú ý***:

* *Đối với các Chi nhánh NHNN****: chỉ nâng cấp TAD\_COMM và CITAD Client.***
* *Đối với các đơn vị khác:* ***Phải thực hiện tuần tự các bước sau (hoàn thành nâng cấp và đăng nhập TAD\_COMM trước sau đó mới tiếp tục nâng cấp TAD\_WEB)***
  + 1. Nâng cấp phiên bản TAD\_COMM
* Download file NangCapPhienBan \_TADCOMM.zip theo link nâng cấp
* Đóng chương trình TAD\_COMM đang chạy.
* Đổi tên thư mục LOGs hiện tại của TAD\_COMM (để backup)
* Giải nén và copy ghi đè vào thư mục cài đặt TAD\_COMM (C:\Program Files ...\SBV\CITAD Communication\)
* Bật TAD\_COMM và đăng nhập hệ thống.
  + 1. Nâng cấp phiên bản TAD\_WEB
* Download file NangCapPhienBan\_TADWEB.zip theo link nâng cấp
* Giải nén và copy đè vào thư mục cài đặt TAD\_WEB (C:\inetpub\wwwroot\CITAD)
* Restart application pool
  + 1. Nâng cấp phiên bản CITAD Client

***Thực hiện trên tất cả các máy có sử dụng CITAD Client:***

* Khi đăng nhập báo sai phiên bản CITAD Client như hình dưới:



* Tải bản cập nhật mới CITAD Client về. (Tên file CITADClientSetup\_v1.0.0.2.msi)
* Đóng chương trình CITAD Client đang bật bằng cách chuột phải biểu tượng ở thanh taskbar (góc phải) chọn Exit.
* Chạy file cài đặt CITADClientSetup\_v1.0.0.2.msi và chạy lại CITAD Client phiên bản mới và truy cập TAD\_WEB

* 1. Hướng dẫn phục hồi phiên bản cũ đang sử dụng

Nếu hệ thống không thể hoạt động được sau khi nâng cấp thì có thể bật máy chủ cài đặt phiên bản cũ lên hoặc phục hồi lại hệ thống để sử dụng. Trước khi thực hiện cần tham khảo ý kiến từ bộ phận hỗ trợ của NHNN

Các bước phục hồi như sau:

* + 1. Phục hồi ứng dụng
       1. Phục hồi chương trình CITAD\_WEB

Phục hồi thư mục CITAD: copy tất cả các file và thư mục con trong thư mục CITAD (đã được backup tại Mục **Backup chương trình CITAD\_WEB**) copy đè vào thư mục CITAD trên máy cài đặt ứng dụng CITAD

* + - 1. Phục hồi chương trình IBPSCommunication

Phục hồi thư mục IBPSCommunication: copy tất cả các file và thư mục con trong thư mục IBPSCommunication (đã được backup tại Mục **Backup chương trình IBPSCommunication**) copy đè vào thư mục IBPSCommunication trên máy cài đặt ứng dụng IBPSCommunication

* + 1. Phục hồi Database

Chương trình phiên bản cũ có thể hoạt động bình thường với Database đã được nâng cấp lên phiên bản 5.0.0.2.0.0 nên sau khi khôi phục lại ứng dụng có thể sử dụng được hệ thống mà không cần phải phục hồi lại Database. Nếu phục hồi Database Đơn vị thành viên cần chú ý có phương án đảm bảo khôi phục cả các dữ liệu phát sinh sau thời điểm backup.

## 

* 1. Khuyến cáo về an ninh bảo mật
     1. Khuyến cáo xóa các file .jar của Tuxedo

| **Component Name** | **Vulnerability** | **Severity** | **Folder** | **File Name** | **Vulnerability Description** |
| --- | --- | --- | --- | --- | --- |
| Apache ActiveMQ | CVE-2010-0684 | Low | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | Cross-site scripting (XSS) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote authenticated users to inject arbitrary web script or HTML via the JMSDestination parameter in a queue action. |
| Apache ActiveMQ | CVE-2010-1244 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | Cross-site request forgery (CSRF) vulnerability in createDestination.action in Apache ActiveMQ before 5.3.1 allows remote attackers to hijack the authentication of unspecified victims for requests that create queues via the JMSDestination parameter in a queue action. |
| Apache ActiveMQ | CVE-2011-4905 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | Apache ActiveMQ before 5.6.0 allows remote attackers to cause a denial of service (file-descriptor exhaustion and broker crash or hang) by sending many openwire failover:tcp:// connection requests. |
| Apache ActiveMQ | CVE-2012-6092 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe messages in webapp/websocket/chat.js.  NOTE: AMQ-4124 is covered by CVE-2012-6551. |
| Apache ActiveMQ | CVE-2012-6551 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests. |
| Apache ActiveMQ | CVE-2013-3060 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests. |
| Apache ActiveMQ | CVE-2015-7559 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | It was found that the Apache ActiveMQ client before 5.15.5 exposed a remote shutdown command in the ActiveMQConnection class. An attacker logged into a compromised broker could use this flaw to achieve denial of service on a connected client. |
| Apache ActiveMQ | CVE-2018-11775 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | apache-activemq-4.1.1.jar | TLS hostname verification when using the Apache ActiveMQ Client before 5.15.6 was missing which could make the client vulnerable to a MITM attack between a Java application using the ActiveMQ client and the ActiveMQ server. This is now enabled by default. |
| Apache Tomcat | CVE-2007-5333 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 6.0.0 through 6.0.14, 5.5.0 through 5.5.25, and 4.1.0 through 4.1.36 does not properly handle (1) double quote (") characters or (2) %5C (encoded backslash) sequences in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks.  NOTE: this issue exists because of an incomplete fix for CVE-2007-3385. |
| Apache Tomcat | CVE-2007-5342 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The default catalina.policy in the JULI logging component in Apache Tomcat 5.5.9 through 5.5.25 and 6.0.0 through 6.0.15 does not restrict certain permissions for web applications, which allows attackers to modify logging configuration options and overwrite arbitrary files, as demonstrated by changing the (1) level, (2) directory, and (3) prefix attributes in the org.apache.juli.FileHandler handler. |
| Apache Tomcat | CVE-2007-6286 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.11 through 5.5.25 and 6.0.0 through 6.0.15, when the native APR connector is used, does not properly handle an empty request to the SSL port, which allows remote attackers to trigger handling of "a duplicate copy of one of the recent requests," as demonstrated by using netcat to send the empty request. |
| Apache Tomcat | CVE-2008-0002 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 6.0.0 through 6.0.15 processes parameters in the context of the wrong request when an exception occurs during parameter processing, which might allow remote attackers to obtain sensitive information, as demonstrated by disconnecting during this processing in order to trigger the exception. |
| Apache Tomcat | CVE-2008-1232 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Cross-site scripting (XSS) vulnerability in Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16 allows remote attackers to inject arbitrary web script or HTML via a crafted string that is used in the message argument to the HttpServletResponse.sendError method. |
| Apache Tomcat | CVE-2008-1947 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Cross-site scripting (XSS) vulnerability in Apache Tomcat 5.5.9 through 5.5.26 and 6.0.0 through 6.0.16 allows remote attackers to inject arbitrary web script or HTML via the name parameter (aka the hostname attribute) to host-manager/html/add. |
| Apache Tomcat | CVE-2008-2370 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16, when a RequestDispatcher is used, performs path normalization before removing the query string from the URI, which allows remote attackers to conduct directory traversal attacks and read arbitrary files via a .. (dot dot) in a request parameter. |
| Apache Tomcat | CVE-2008-2938 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Directory traversal vulnerability in Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16, when allowLinking and UTF-8 are enabled, allows remote attackers to read arbitrary files via encoded directory traversal sequences in the URI, a different vulnerability than CVE-2008-2370.  NOTE: versions earlier than 6.0.18 were reported affected, but the vendor advisory lists 6.0.16 as the last affected version. |
| Apache Tomcat | CVE-2008-5515 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalizes the target pathname before filtering the query string when using the RequestDispatcher method, which allows remote attackers to bypass intended access restrictions and conduct directory traversal attacks via .. (dot dot) sequences and the WEB-INF directory in a Request. |
| Apache Tomcat | CVE-2009-0033 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when the Java AJP connector and mod\_jk load balancing are used, allows remote attackers to cause a denial of service (application outage) via a crafted request with invalid headers, related to temporary blocking of connectors that have encountered errors, as demonstrated by an error involving a malformed HTTP Host header. |
| Apache Tomcat | CVE-2009-0580 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when FORM authentication is used, allows remote attackers to enumerate valid usernames via requests to /j\_security\_check with malformed URL encoding of passwords, related to improper error checking in the (1) MemoryRealm, (2) DataSourceRealm, and (3) JDBCRealm authentication realms, as demonstrated by a % (percent) value for the j\_password parameter. |
| Apache Tomcat | CVE-2009-0781 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 allows remote attackers to inject arbitrary web script or HTML via the time parameter, related to "invalid HTML." |
| Apache Tomcat | CVE-2009-0783 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 permits web applications to replace an XML parser used for other web applications, which allows local users to read or modify the (1) web.xml, (2) context.xml, or (3) tld files of arbitrary web applications via a crafted application that is loaded earlier than the target application. |
| Apache Tomcat | CVE-2009-2693 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in an entry in a WAR file, as demonstrated by a ../../bin/catalina.bat entry. |
| Apache Tomcat | CVE-2009-2901 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The autodeployment process in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20, when autoDeploy is enabled, deploys appBase files that remain from a failed undeploy, which might allow remote attackers to bypass intended authentication requirements via HTTP requests. |
| Apache Tomcat | CVE-2009-2902 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to delete work-directory files via directory traversal sequences in a WAR filename, as demonstrated by the ...war filename. |
| Apache Tomcat | CVE-2009-3548 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges. |
| Apache Tomcat | CVE-2010-1157 | Low | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource that requires (1) BASIC or (2) DIGEST authentication, and then reading the realm field in the WWW-Authenticate header in the reply. |
| Apache Tomcat | CVE-2010-2227 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 through 6.0.27, and 7.0.0 beta does not properly handle an invalid Transfer-Encoding header, which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header that interferes with "recycling of a buffer." |
| Apache Tomcat | CVE-2010-3718 | Low | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 7.0.0 through 7.0.3, 6.0.x, and 5.5.x, when running within a SecurityManager, does not make the ServletContext attribute read-only, which allows local web applications to read or write files outside of the intended working directory, as demonstrated using a directory traversal attack. |
| Apache Tomcat | CVE-2010-4172 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Multiple cross-site scripting (XSS) vulnerabilities in the Manager application in Apache Tomcat 6.0.12 through 6.0.29 and 7.0.0 through 7.0.4 allow remote attackers to inject arbitrary web script or HTML via the (1) orderBy or (2) sort parameter to sessionsList.jsp, or unspecified input to (3) sessionDetail.jsp or (4) java/org/apache/catalina/manager/JspHelper.java, related to use of untrusted web applications. |
| Apache Tomcat | CVE-2010-4312 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The default configuration of Apache Tomcat 6.x does not include the HTTPOnly flag in a Set-Cookie header, which makes it easier for remote attackers to hijack a session via script access to a cookie. |
| Apache Tomcat | CVE-2011-0013 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Multiple cross-site scripting (XSS) vulnerabilities in the HTML Manager Interface in Apache Tomcat 5.5 before 5.5.32, 6.0 before 6.0.30, and 7.0 before 7.0.6 allow remote attackers to inject arbitrary web script or HTML, as demonstrated via the display-name tag. |
| Apache Tomcat | CVE-2011-0534 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 7.0.0 through 7.0.6 and 6.0.0 through 6.0.30 does not enforce the maxHttpHeaderSize limit for requests involving the NIO HTTP connector, which allows remote attackers to cause a denial of service (OutOfMemoryError) via a crafted request. |
| Apache Tomcat | CVE-2011-1184 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values. |
| Apache Tomcat | CVE-2011-2204 | Low | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file. |
| Apache Tomcat | CVE-2011-2526 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.19, when sendfile is enabled for the HTTP APR or HTTP NIO connector, does not validate certain request attributes, which allows local users to bypass intended file access restrictions or cause a denial of service (infinite loop or JVM crash) by leveraging an untrusted web application. |
| Apache Tomcat | CVE-2011-3190 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request. |
| Apache Tomcat | CVE-2011-4084 |  | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | \*\* REJECT \*\*  DO NOT USE THIS CANDIDATE NUMBER.  ConsultIDs: CVE-2011-4858.  Reason: This candidate is a duplicate of CVE-2011-4858.  Notes: All CVE users should reference CVE-2011-4858 instead of this candidate.  All references and descriptions in this candidate have been removed to prevent accidental usage. |
| Apache Tomcat | CVE-2011-4858 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat before 5.5.35, 6.x before 6.0.35, and 7.x before 7.0.23 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters. |
| Apache Tomcat | CVE-2011-5062 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check qop values, which might allow remote attackers to bypass intended integrity-protection requirements via a qop=auth value, a different vulnerability than CVE-2011-1184. |
| Apache Tomcat | CVE-2011-5063 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check realm values, which might allow remote attackers to bypass intended access restrictions by leveraging the availability of a protection space with weaker authentication or authorization requirements, a different vulnerability than CVE-2011-1184. |
| Apache Tomcat | CVE-2011-5064 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | DigestAuthenticator.java in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 uses Catalina as the hard-coded server secret (aka private key), which makes it easier for remote attackers to bypass cryptographic protection mechanisms by leveraging knowledge of this string, a different vulnerability than CVE-2011-1184. |
| Apache Tomcat | CVE-2012-0022 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling parameters, which allows remote attackers to cause a denial of service (CPU consumption) via a request that contains many parameters and parameter values, a different vulnerability than CVE-2011-4858. |
| Apache Tomcat | CVE-2012-2733 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO connector in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28 does not properly restrict the request-header size, which allows remote attackers to cause a denial of service (memory consumption) via a large amount of header data. |
| Apache Tomcat | CVE-2012-3544 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2012-3546 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2012-4431 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2012-4534 | Low | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2012-5568 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris. |
| Apache Tomcat | CVE-2012-5885 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and nc (aka nonce-count) values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, a different vulnerability than CVE-2011-1184. |
| Apache Tomcat | CVE-2012-5886 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 caches information about the authenticated user within the session state, which makes it easier for remote attackers to bypass authentication via vectors related to the session ID. |
| Apache Tomcat | CVE-2012-5887 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 does not properly check for stale nonce values in conjunction with enforcement of proper credentials, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests. |
| Apache Tomcat | CVE-2013-4286 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2013-4322 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2013-4590 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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. |
| Apache Tomcat | CVE-2014-0075 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data. |
| Apache Tomcat | CVE-2014-0096 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. |
| Apache Tomcat | CVE-2014-0099 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header. |
| Apache Tomcat | CVE-2014-0119 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | 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 the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application. |
| Apache Tomcat | CVE-2014-0227 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle attempts to continue reading data after an error has occurred, which allows remote attackers to conduct HTTP request smuggling attacks or cause a denial of service (resource consumption) by streaming data with malformed chunked transfer coding. |
| Apache Tomcat | CVE-2014-0230 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (thread consumption) via a series of aborted upload attempts. |
| Apache Tomcat | CVE-2014-7810 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The Expression Language (EL) implementation in Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.58, and 8.x before 8.0.16 does not properly consider the possibility of an accessible interface implemented by an inaccessible class, which allows attackers to bypass a SecurityManager protection mechanism via a web application that leverages use of incorrect privileges during EL evaluation. |
| Apache Tomcat | CVE-2015-5174 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Directory traversal vulnerability in RequestUtil.java in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.65, and 8.x before 8.0.27 allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application in a getResource, getResourceAsStream, or getResourcePaths call, as demonstrated by the $CATALINA\_BASE/webapps directory. |
| Apache Tomcat | CVE-2015-5345 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The Mapper component in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.30, and 9.x before 9.0.0.M2 processes redirects before considering security constraints and Filters, which allows remote attackers to determine the existence of a directory via a URL that lacks a trailing / (slash) character. |
| Apache Tomcat | CVE-2016-0706 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 does not place org.apache.catalina.manager.StatusManagerServlet on the org/apache/catalina/core/RestrictedServlets.properties list, which allows remote authenticated users to bypass intended SecurityManager restrictions and read arbitrary HTTP requests, and consequently discover session ID values, via a crafted web application. |
| Apache Tomcat | CVE-2016-0714 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The session-persistence implementation in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 mishandles session attributes, which allows remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context via a web application that places a crafted object in a session. |
| Apache Tomcat | CVE-2016-0762 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder. |
| Apache Tomcat | CVE-2016-5018 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications. |
| Apache Tomcat | CVE-2016-5388 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP\_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability. |
| Apache Tomcat | CVE-2016-6794 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible. |
| Apache Tomcat | CVE-2016-6796 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet. |
| Apache Tomcat | CVE-2016-6797 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not. |
| Apache Tomcat | CVE-2016-6816 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own. |
| Apache Tomcat | CVE-2016-8735 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types. |
| Apache Tomcat | CVE-2017-5647 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | catalina-6.0.14.jar | A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. |
| Apache-XML Xml Security | CVE-2013-2153 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | The XML digital signature functionality (xsec/dsig/DSIGReference.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows context-dependent attackers to reuse signatures and spoof arbitrary content via crafted Reference elements in the Signature, aka "XML Signature Bypass issue." |
| Apache-XML Xml Security | CVE-2013-2154 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | Stack-based buffer overflow in the XML Signature Reference functionality (xsec/dsig/DSIGReference.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions, probably related to the DSIGReference::getURIBaseTXFM function. |
| Apache-XML Xml Security | CVE-2013-2155 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 does not properly validate length values, which allows remote attackers to cause a denial of service or bypass the CVE-2009-0217 protection mechanism and spoof a signature via crafted length values to the (1) compareBase64StringToRaw, (2) DSIGAlgorithmHandlerDefault, or (3) DSIGAlgorithmHandlerDefault::verify functions. |
| Apache-XML Xml Security | CVE-2013-2156 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | Heap-based buffer overflow in the Exclusive Canonicalization functionality (xsec/canon/XSECC14n20010315.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PrefixList attribute. |
| Apache-XML Xml Security | CVE-2013-2210 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | Heap-based buffer overflow in the XML Signature Reference functionality in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions.  NOTE: this is due to an incorrect fix for CVE-2013-2154. |
| Apache-XML Xml Security | CVE-2013-4517 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | xmlsec-1.4.0.jar | Apache Santuario XML Security for Java before 1.5.6, when applying Transforms, allows remote attackers to cause a denial of service (memory consumption) via crafted Document Type Definitions (DTDs), related to signatures. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-1523 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Directory traversal vulnerability in the HTTP server in Mort Bay Jetty 5.1.14, 6.x before 6.1.17, and 7.x through 7.0.0.M2 allows remote attackers to access arbitrary files via directory traversal sequences in the URI. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-1524 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Cross-site scripting (XSS) vulnerability in Mort Bay Jetty before 6.1.17 allows remote attackers to inject arbitrary web script or HTML via a directory listing request containing a ; (semicolon) character. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-4609 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | The Dump Servlet in Mort Bay Jetty 6.x and 7.0.0 allows remote attackers to obtain sensitive information about internal variables and other data via a request to a URI ending in /dump/, as demonstrated by discovering the value of the getPathTranslated variable. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-4610 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Multiple cross-site scripting (XSS) vulnerabilities in Mort Bay Jetty 6.x and 7.0.0 allow remote attackers to inject arbitrary web script or HTML via (1) the query string to jsp/dump.jsp in the JSP Dump feature, or the (2) Name or (3) Value parameter to the default URI for the Session Dump Servlet under session/. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-4611 | High | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Mort Bay Jetty 6.x through 6.1.22 and 7.0.0 writes backtrace data without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator, related to (1) a string value in the Age parameter to the default URI for the Cookie Dump Servlet in test-jetty-webapp/src/main/java/com/acme/CookieDump.java under cookie/, (2) an alphabetic value in the A parameter to jsp/expr.jsp, or (3) an alphabetic value in the Content-Length HTTP header to an arbitrary application. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-4612 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Multiple cross-site scripting (XSS) vulnerabilities in the WebApp JSP Snoop page in Mort Bay Jetty 6.1.x through 6.1.21 allow remote attackers to inject arbitrary web script or HTML via the PATH\_INFO to the default URI under (1) jspsnoop/, (2) jspsnoop/ERROR/, and (3) jspsnoop/IOException/, and possibly the PATH\_INFO to (4) snoop.jsp. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-5048 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Cookie Dump Servlet stored XSS vulnerability in jetty though 6.1.20. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2009-5049 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | WebApp JSP Snoop page XSS in jetty though 6.1.21. |
| Cometd - org.mortbay.jetty:cometd-demo | CVE-2011-4461 | Medium | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | jetty-6.1.7.jar | Jetty 8.1.0.RC2 and earlier computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters. |
| Cometd - org.mortbay.jetty:cometd-demo |  |  | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | log4j-1.2.12.jar |  |
| Cometd - org.mortbay.jetty:cometd-demo |  |  | tuxedo12.1.1.0\_VS2010/udataobj/salt/sca/tuscany/lib | annotations-api-6.0.14.jar |  |