ÍNDEX

Versió	Redactat / revisat per	Aprovat per	Data aprovació	Data publicació
1.0.	CTTI – Qualitat i Seguretat	Comitè de Direcció del CTTI	26/05/2006	01/06/2006
2.0	CTTI -- QSRaP	CTTI – QSRaP	5/10/2009	6/10/2009

Estàndard signat digitalment pel:

Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2009.10.06 12:16:27 +02'00'

RESPONSABLE DEL DOCUMENT: CTTI – Qualitat, Seguretat i Relació amb Proveïdors

RESUM

OBJECTIU

Definir els controls a aplicar per a la protecció d'equips instal·lats amb el servidor d'aplicacions *Tomcat*, amb l'objectiu de garantir la confidencialitat, integritat i disponibilitat de la informació i serveis suportats per aquesta plataforma.

ÀMBIT

Servidors d'aplicacions *Tomcat* de la Generalitat de Catalunya.

DESCRIPCIÓ

Es recullen els controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació de sistemes basat en *Tomcat*.

1 OBJECTIU

Definir els controls per a instal·lar, configurar, mantenir i explotar el servidor d'aplicacions *Apache Tomcat* d'una manera segura, que garanteixi la confidencialitat, integritat i disponibilitat dels serveis web implantats amb aquesta plataforma a la Generalitat de Catalunya.

No és l'objectiu d'aquesta guia, la definició i programació d'aplicacions *JSP* i *servlets* de forma segura.

Tots els canvis proposats en aquesta guia han de ser primer instal·lats en un entorn de desenvolupament i s'ha fer un test exhaustiu de les aplicacions per tal d'assegurar que tot continua funcionant normalment.

2 ÀMBIT I VIGÈNCIA

Aquesta guia va destinada als administradors i responsables d'instal·lació, explotació i manteniment dels servidors d'aplicacions *Apache Tomcat* de la Generalitat de Catalunya, per tal que aquests, basant-se en una anàlisi dels potencials riscos de seguretat, puguin triar els controls més adients a les particularitats de l'organització a la que s'està donant servei.

En el cas que el manteniment dels servidors estigui externalitzat, caldrà exigir per contracte l'aplicació dels controls de seguretat.

La versió actual entrarà en vigor el dia 6 d'octubre de 2009.

Aquesta guia romandrà vigent fins la propera versió aprovada de la mateixa.

3 COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

La present guia proporciona cobertura a aspectes recollits en els següents controls de la ISO 27002:2005:

- 6.2.3 Requeriments de seguretat en els acords amb les terceres parts
- 9.2.1 Ubicació i protecció dels equips
- 10.10.1 Registres d'auditoria (logging)
- 11.4.4 Protecció dels ports de configuració i diagnòstic remot
- 11.5.1 Processos de connexió segurs
- 11.6.1 Restricció d'accés a la informació
- 11.6.2 Aïllament de sistemes sensibles
- 12.5.3 Restriccions en els canvis als paquets de programari
- 13.1.1 Notificar dels esdeveniments de seguretat

4 DESCRIPCIÓ DELS CONTROLS

Es presenten a continuació els possibles controls de seguretat orientats a garantir la confidencialitat, privacitat, integritat i disponibilitat de la informació, així com el compliment de la legislació vigent. Aquests s'agrupen per grups d'accions o procediments operatius orientats a combatre les amenaces a les quals un entorn d'aplicacions està exposat. Sota la columna "categoria", s'especifiquen els aspectes de seguretat que cada control reforça (confidencialitat– C, integritat– I, disponibilitat– D).

4.1. IN - Instal·lació i manteniment

OBJECTIUS	
Requisits en la instal·lació, actualització i manteniment del servidor d'aplicacions *Tomcat*. Els controls apliquen a entorns de producció.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C1. Mantenir actualitzat el servidor d'aplicacions amb els pegats de seguretat adequats. Pels sistemes ubicats en l'àmbit dels Serveis TIC Centrals, cal donar compliment a la *Norma de gestió de vulnerabilitats de programari base*.	I D
C2. Durant la instal·lació inicial de *Tomcat*, no seleccionar les aplicacions d'exemple i, en cas que la seva instal·lació sigui obligatòria, esborrar-los després de la instal·lació.	I D

C3. No instal·lar Tomcat en servidors de bases de dades o controladors de domini.	C I D
C4. S'han de revisar els riscos associats a la instal·lació de mòduls, *plug-ins* o pegats de terceres parts, tenint en compte les vulnerabilitats que es poden introduir.	C I D
C5. No utilitzar en entorns d'explotació els certificats SSL creats per entorns de proves o pre-producció.	D
C6. Configurar el mòdul *SSL mod_ssl* per a poder utilitzar *HTTPS* per accedir al servidor web si és necessari. Utilitzar protocols robustos SSL v3 i TLS v1 i claus de com a mínim 128 bits	C I
C7. Protegir el sistema operatiu, controlant els serveis de xarxa que té habilitats. Cal mantenir el sistema operatiu al dia dels pegats de seguretat. (Veure *Guia protecció entorns Linux, Solaris, AIX, HP-UX, Windows 2003*).	C I D
C8. Crear un usuari en el sistema per a l'execució del servidor *Tomcat* amb els següents requisits: • Privilegis d'accés a la carpeta on està instal·lat *Tomcat*. • Permisos de lectura, escriptura i execució a la carpeta <*tomcat_home*>, a l'arbre de directoris de *Tomcat* i els directoris de domini on resideixen les aplicacions i fitxers de configuració. • No ha de tenir privilegis d'administració sobre el sistema operatiu.	I D
C9. Si s'instal·la el servidor d'aplicacions com a servei perquè s'inicii automàticament durant el procés d'arrencada del servidor, configurar que ho faci amb l'usuari definit per a l'execució de *Tomcat*.	C I D
C10. Actualitzar les versions dels connectors web utilitzats, per disminuir el risc d'atac utilitzant les possibles vulnerabilitats dels connectors.	C I D
C11. Si existeix un conjunt de servidors *Tomcat* donant servei (*cluster*), protegir de possibles intrusions les comunicacions privades de replicació entre els servidors.	C I D
C12. Caldrà donar compliment a la *Norma de còpies de seguretat* per a garantir que es realitza còpia de seguretat dels sistemes.	C I D

4.2. CN - Configuració

OBJECTIUS	
Configurar la instal·lació del servidor d'aplicacions *Tomcat* per a garantir la seguretat dels serveis web que presten, així com indicar la configuració de les aplicacions a desplegar.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C13. Protegir el fitxer <*tomcat_home*>*/conf/server.xml* d'accessos d'usuaris, ja que només l'administrador de *Tomcat* ho ha de poder llegir.	C I
C14. L'opció *reloadable* al fitxer de desplegament de l'aplicació (*web.xml*), molt útil en sistemes de prova o desenvolupament, serveix per activar la càrrega automàtica de classes dintre del context d'una aplicació. No obstant això, cal desactivar-la en sistemes en explotació.	D
C15. Si la versió de *Tomcat* és 4 o superior, utilitzar algun *realm* per demanar autenticació en accedir a continguts dinàmics que només hagin de ser accessibles per determinats usuaris. S'ha d'afegir la corresponent directiva *realm* al fitxer *server.xml*, la directiva de restricció de seguretat al fitxer de desplegament de l'aplicació *web.xml* i crear el fitxer *tomcat-users.xml* si la base de dades d'usuaris i rols és local (en aquest cas es tracta d'un *MemoryRealm*).	C I
C16. Cal donar compliment a la *Norma de gestió de comptes d'administració de sistemes* per a garantir la correcta definició i gestió dels comptes amb privilegis d'administració.	C I D

Recomanacions

R1. Utilitzar *Security Manager*, una utilitzat de *Tomcat* que serveix per protegir les aplicacions desplegades de *servlets* i *JSPs* troians o inclús d'errors de programació.

R2. Provar les configuracions de seguretat en un entorn de proves abans d'aplicar-les en servidors que estiguin en explotació.

R3. Configurar les pàgines a mostrar en cas d'error del servidor d'aplicacions, evitant que siguin per defecte les del servidor i evitant donar informació sobre el producte, la versió o qualsevol altra que pugui servir per vulnerar el sistema. Per a fer-ho cal configurar el paràmetre <*error-page*> en el descriptor d'aplicació *web.xml*.

R4. Restringir la longitud i el temps límit de les peticions web contra el servidor d'aplicacions per a evitar atacs de denegació de servei.

R5. Limitar el número de connexions obertes i el número de processos permesos en el servidor. D'aquesta manera es protegeixen contra atacs de denegació de servei intentant esgotar els recursos de processament de peticions del servidor o d'un mal ús que en facin les aplicacions desplegades.

R6. Evitar que en les respostes *HTTP* als clients o en els missatges de benvinguda s'informi del producte o de la versió del servidor d'aplicacions.

4.3. MN - Monitoratge

OBJECTIUS	
Registrar tots els intents d'accés a *Tomcat* per tal de poder conduir futures investigacions en cas de necessitat i atribuir-ne responsabilitats.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C17. Caldrà donar compliment als requeriments de la *Norma de gestió de traces* per a garantir la traçabilitat i custòdia dels esdeveniments dels sistemes.	C I
C18. Pels sistemes d'àmbit departament / ens, es connectaran a eines de correlació de traces pròpies quan existeixin; de no ser així, caldrà guardar les traces durant un període mínim d'un any i revisar-les periòdicament per a detectar anomalies o incidències en el funcionament del sistema.	C I
C19. Qualsevol possible incident de seguretat haurà de ser comunicat en la major brevetat possible mitjançant el *Procediment de notificació d'incidents de seguretat*.	C I
C20. Protegir els fitxers de traces que genera *Tomcat* contra modificacions d'usuaris o processos mal intencionats.	C I D

Recomanacions

R7. Es recomana, revisar periòdicament les traces per a detectar activitats anòmales que puguin comprometre la seguretat del sistema

4.4. IA - Identificació i Autenticació

OBJECTIUS	
Identificar i autenticar correctament als usuaris que accedeixen a una aplicació desplegada en *Tomcat*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C21. A l'hora de crear un usuari amb rol *manager* per accedir al *Security Manager*, adjudicar-li una clau robusta i no permetre l'accés a l'eina des de l'exterior per tal d'evitar accessos no autoritzats. Inclús es poden fer servir les directives adequades per limitar l'accés a l'eina des d'una llista concreta de clients.	C I D

Recomanacions

R8. Dintre del context de l'aplicació, al fitxer *web.xml* amb les directives de desplegament, utilitzar *RemoteHostValve* i *RemoteAddrValve* per limitar els clients als quals *Tomcat* servirà continguts, per nom o per adreça IP, respectivament.

4.5. AU - Auditoria

OBJECTIUS	
Controlar la configuració dels servidors d'aplicacions *Tomcat*, i analitzar esdeveniments registrats que poguessin suposar una amenaça per la seguretat, identificant àrees vulnerables.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C22. Caldrà facilitar les tasques d'auditoria per part de l'Oficina de Seguretat davant a la revisió del compliment dels requeriments de seguretat marcats pel CTTI.	C I D

4.6. OU - Outsourcing o subcontractació del servei

OBJECTIUS	
Garantir l'acompliment de les mesures de seguretat i dels acords de nivell de servei en cas de subcontractació o externalització del servei de manteniment dels servidors d'aplicacions *Tomcat*.	
CARACTERÍSTIQUES	
Descripció	**Categoria**
C23. Es recollirà contractualment el compliment de les normes i guies que el CTTI tingui per als servidors d'aplicacions *Tomcat* així com qualsevol altre norma de gestió o administració que sigui d'aplicació.	C I D
C24. Garantir el compliment de la *Norma de contractació de Tercers*.	C I D
C25. Garantir la qualitat i el nivell de servei requerit, a través d'acords de nivell de servei: • Procediments d'escalat d'incidències. • Temps de resolució d'incidències. • Temps de resposta per canvis / noves instal·lacions. • Compliment i actualització dels controls de seguretat. • Gestió de problemes. • Etc... L'incompliment d'acords de nivell de servei haurà de comportar penalitzacions econòmiques al proveïdor.	C I D

5 CONTROL

Per a l'àmbit dels *Serveis TIC Centrals*, el control del compliment d'aquesta guia es realitzarà mitjançant auditories periòdiques segons s'estableix en el *Pla d'auditories de seguretat*. Per altres àmbits, es recomana realitzar auditories cada 6 mesos.

En el cas de què no s'apliqui algun dels controls d'aquesta guia, caldrà justificar i documentar aquestes excepcions. Per a l'àmbit dels *Serveis TIC Centrals*, cada excepció a un control haurà de ser autoritzada prèviament per l'Oficina de Seguretat.

Caldrà mantenir un registre on quedin recollides totes les excepcions, a disposició de les auditories.

6 PENALITZACIONS

Quan l'explotació / manteniment dels sistemes estigui subcontractat, en cas d'incompliment aplicaran les penalitzacions recollides en el contracte de la prestació del servei.

Si l'administració del sistema recau en personal intern de la Generalitat de Catalunya, l' incompliment d'aquesta guia pot determinar, si s'escau, l'aplicació del règim disciplinari corresponent.

7 DIVULGACIÓ

L'àrea de Qualitat, Seguretat i Relacions amb Proveïdors del CTTI publicarà aquesta guia al repositori d'estàndards de la intranet del CTTI.

8 REVISIÓ

Aquesta guia ha de ser revisada anualment.

En cas de produir-se una incidència de seguretat relacionada amb aquesta guia, caldrà fer una revisió de compliment i completesa.

9 GLOSSARI DE TERMES

HTTPS: *HTTP* sobre *SSL*. Protocol de transmissió segura de contingut web.

JSP: *Java Server Page*. Tecnologia per a controlar el contingut i aparença de les pàgines web usant servlets. Permeten que la pàgina sigui construïda dinàmicament abans de ser enviada al servidor.

NAT: *Network Address Translation*. Traduir adreces IP usades en una xarxa a unes altres adreces IP conegudes en una altra xarxa.

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

Servlet: Programa que s'executa en el servidor per realitzar accions que generalment generen una resposta per enviar al client web.

Socket: Canal de comunicació amb un equip per a la prestació d'un servei a través d'un port.

Realm: Conjunt de directives a un JSP per crear un entorn o context d'aplicació segur, indicant usuaris, rols, mètodes d'autenticació, etc.

10 DOCUMENTACIÓ REFERENCIADA

- GE-GUI07 Guia protecció entorns Linux
- GE-GUI08 Guia protecció entorns Solaris
- GE-GUI27 Guia de protecció entorns HP-UX
- GE-GUI32 Guia proteccio entorns AIX
- GE-GUI10 Guia protecció entorns Windows 2003
- GE-GUI40 Guia de còpies de seguretat
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- GE-GUI19 Guia de contrasenyes
- GE-GUI20 Guia de gestió de comptes d'administrador de sistemes
- CT-NOR03 Norma de contractació de tercers
- GE-PRO01 Procediment de notificació d'incidents de seguretat
- Pla d'auditories de seguretat

- Documentació:
  - *Tomcat 4 Security Manager How-To* (http://tomcat.apache.org/tomcat-4.1-doc/security-manager-howto.html)
  - Guia d'aprenentatge de *Tomcat* (http://www.programacion.com/tutorial/tomcatintro)
  - *Tomcat 4 Security Realms* (http://www.onjava.com/pub/a/onjava/2001/07/24/tomcat.html)
  - *Realm Configuration How-To* (http://tomcat.apache.org/tomcat-4.0-doc/realm-howto.html)

- *Security Manager Configuration How-To* (http://tomcat.apache.org/tomcat-4.0-doc/manager-howto.html)
- Guia de *Tomcat* (http://tomcatbook.sourceforge.net/book/defaulthtml/index.html)
- Informació general de *Tomcat* (http://tomcat.apache.org)
- *Tomcat 5.5 Security Manager How-To* (http://tomcat.apache.org/tomcat-5.5-doc/security-manager-howto.html)
- *Tomcat 5.5 Manager How-To* (http://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html)
- *Tomcat 5.5 Security Realms How-To* (http://tomcat.apache.org/tomcat-5.5-doc/realm-howto.html#What%20is%20a%20Realm?)

Eines

- Servidor CAMS (*Cafésoft Access Management System*). Utilitat que disposa d'algunes de les següents característiques, no disponibles a *Tomcat* per sí mateix (consultar http://www.cafesoft.com/products/cams/access-management-white-paper.html per més informació):
  - Autenticació per adreça IP.
  - Autenticació per limitació en el temps (franja horària).
  - Autenticació una única vegada (*Single sing-on*).
  - Aplicar mesures de seguretat de manera centralitzada i no individualment per cada aplicació desplegada.
  - Registrar els accessos autoritzats o no de certs usuaris a certes aplicacions.
  - Disposar d'un fitxer de traces comú a totes les aplicacions desplegades en comptes d'un fitxer de traces per cada aplicació.

11 PARAULES CLAU

Servidor d'aplicacions, desplegament, directives, rols, servlet, JSP, https, Tomcat, hardenning, protecció.

12 HISTÒRIC DEL DOCUMENT

Versió 1.0
Versió inicial.

Versió 2.0
Versió revisada de l'estàndard. Veure la fitxa de l'estàndard per a més informació.