Jetty Security

Jetty Security Reports

Resolved Issues

Date	ID	Exploitable	Severity	Affects	Fixed Version	Comment
5/11/2009	CERT120541/CVE-2009-3555	medium	**high**	JVM < 1.6 u19	jetty-7.0.1.v20091125,jetty-6.1.22	Work around by turning off SSL renegotiation in Jetty. If using JVM > 1.6u19 setAllowRenegotiate(true) may be called on connectors
1/7/2009	JETTY-1042	low	high	<=6.1.18, <=7.0.0.M4	6.1.19, 7.0.0.Rc0	cookie leak between requests sharing a connection
30/04/2009	CERT402580	medium	**high**	<=6.1.16,<=7.0.0.M2	5.1.15,6.1.18, 7.0.0.M2 JETTY-1004	view arbitrary disk content in some specific configurations
22/12/2007	CVE-2007-6672/CERT553235	**high**	medium	6.1.rrc0-6.1.6	6.1.7 see JETTY-386	Static content visible in WEB-INF and past security constraints
5/11/2007	CVE-2007-5614/CERT438616	low	low	<6.1.6	6.1.6rc1 (patch in CVS for jetty5)	Singled quote in cookie name
5/11/2007	CVE-2007-5613/CERT237888	low	low	<6.1.6	6.1.6rc1 (patch in CVS for jetty5)	XSS in demo dump servlet

3/10/2007	CVE-2007-5615/CERT21284	medium	medium	<6.1.6	6.1.6rc0 (patch in CVS for jetty5)	CRLF Response splitting
22/11/2006	CVE-2006-6969	low	**high**	<6.1.0,<6.0.2, <5.1.12,<4.2.27	6.1.0pre3, 6.0.2, 5.1.12, 4.2.27	Session ID predictability
1/6/2006	CVE-2006-2759	medium	medium	6.0.*<6.0.0Beta17	6.0.0Beta17	JSP source visibility
5/1/2006		medium	medium	<5.1.10	5.1.10	Fixed // security constraint bypass on windows
18/11/2005	CVE-2006-2758	medium	medium	<5.1.6	5.1.6, 6.0.0Beta4	JSP source visibility
4/2/2004	JSSE 1.0.3_01	medium	medium	<4.2.7	4.2.7	Upgraded JSSE to obtain downstream security fix
22/9/2002		**high**	**high**	<4.1.0	4.1.0	Fixed CGI servlet remove exploit
12/3/2002		medium		<3.1.7	4.0.RC2, 3.1.7	Fixed // security constraint bypass
21/10/2001		medium		< 3.1.3	3.1.3	Fixed trailing null security constraint bypass

Known Jetty 6 Issues

none

Known Jetty 5 Issues

CVE-2007-5613/CERT237888 - The demonstration Dump servlet is vulnerable to cross site scripting. The Dump servlet from jetty 5 should not be deployed on production sites.

CVE-2007-5614/CERT438616 - HTTP Cookie names are not checked for illegal characters. Unvalidated user data should not be used as the basis of a cookie name in an application served by Jetty 5.

CVE-2007-5615/CERT21284 - The HTTP header names and values set by an application are not checked for illegal characters. Unvalidated user data should not be used for either a HTTP header name or a HTTP header value.