Open Source Vulnerability Report

BLACKDUCK

Duck Hub Demo > 2.0

Phase: RELEASED | Distribution: EXTERNAL

Vulnerability Status Filter: All Vulnerabilities

44 HIGH	115 MEDIUM	10 LOW

VULNERABLE COMPONENTS SUMMARY

Apache Commons FileUpload 1.2.2	3	0	2
Apache HttpComponents Client 4.2.5	0	2	0
Apache POI 3.8	1	4	0
Apache Struts 2.3.7	30	22	0
Apache Xalan (Java) 2.7.1	1	0	0
Apache Xerces2 J 2.6.2	1	0	0
Hibernate Validator 4.1.0.Final	0	1	0
Jersey 1.13	0	1	0
Jetty: Java based HTTP, Servlet, SPDY, WebSocket Server 6.0.1	6	71	8
Spring Framework 3.0.0	2	8	0
Spring Security 3.0.0.RELEASE	0	5	0

VULNERABLE COMPONENTS DETAILS

Apache Commons FileUpload 1.2.2

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
90906	LOW	3.3	4.9	3.4	DUPLICATE	02/16/2017
Apache Commons FileUpload contains a flaw as the program creates temporary files insecurely. It is possible for a local attacker to use a symlink attack against files temporarily stored in /tmp, due to predictable filenames, to cause the program to unexpectedly overwrite an arbitrary file.						
98703	HIGH	7.5	6.4	10.0	REMEDIATION COMPLETE	09/01/2016
Apache Commons contains a flaw in the DiskFileItem class. This issue is triggered during the handling of NULL characters. This may allow a remote attacker to upload arbitrary files by supplying a serialized instance of the DiskFileItem class.						
CVE-2013-0248	LOW	3.3	4.9	3.4	NEW	11/28/2016
The default configuration of javax.servlet.context.tempdir in Apache Commons FileUpload 1.0 through 1.2.2 uses the /tmp directory for uploaded files, which allows local users to overwrite arbitrary files via an unspecified symlink attack.						
CVE-2014-0050	HIGH	7.5	6.4	10.0	NEEDS REVIEW	02/16/2017
MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted Content-Type header that bypasses a loop's intended exit conditions.						
CVE-2016-3092	HIGH	7.8	6.9	10.0	NEW	11/28/2016
The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.						

Apache HttpComponents Client 4.2.5

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2014-3577	MEDIUM	5.8	4.9	8.6	NEW	01/10/2017
org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.						
CVE-2015-5262	MEDIUM	4.3	2.9	8.6	NEW	10/28/2015
http/conn/ssl/SSLConnectionSocketFactory.java in Apache HttpComponents HttpClient before 4.3.6 ignores the http.socket. timeout configuration setting during an SSL handshake, which allows remote attackers to cause a denial of service (HTTPS call hang) via unspecified vectors.						

Apache POI 3.8

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2012-0213	MEDIUM	5.0	2.9	10.0	NEW	02/10/2017
The UnhandledDataStructure function in hwpf/model/UnhandledDataStructure.java in Apache POI 3.8 and earlier allows remote attackers to cause a denial of service (OutOfMemoryError exception and possibly JVM destabilization) via a crafted length value in a Channel Definition Format (CDF) or Compound File Binary Format (CFBF) document.						
CVE-2014-3529	MEDIUM	4.3	2.9	8.6	NEW	02/10/2017
The OPC SAX setup in Apache POI before 3.10.1 allows remote attackers to read arbitrary files via an OpenXML file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.						
CVE-2014-3574	MEDIUM	4.3	2.9	8.6	NEW	02/10/2017
Apache POI before 3.10.1 and 3.11.x before 3.11-beta2 allows remote attackers to cause a denial of service (CPU consumption and crash) via a crafted OOXML file, aka an XML Entity Expansion (XEE) attack.						
CVE-2016-5000	MEDIUM	4.3	2.9	8.6	REMEDIATION COMPLETE	02/10/2017
The XLSX2CSV example in Apache POI before 3.14 allows remote attackers to read arbitrary files via a crafted OpenXML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.						
CVE-2017-5644	HIGH	7.1	6.9	8.6	NEW	03/28/2017
Apache POI in versions prior to release 3.15 allows remote attackers to cause a denial of service (CPU consumption) via a specially crafted OOXML file, aka an XML Entity Expansion (XEE) attack.						

Apache Struts 2.3.7

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
103918	HIGH	10.0	10.0	10.0	DUPLICATE	01/12/2017
Apache Commons FileUpload contains flaw that is due to ParametersInterceptor allowing access to the 'class' parameter. This may allow a remote attacker to manipulate the ClassLoader and execute arbitrary Java code.						
93646	MEDIUM	6.8	6.4	8.6	DUPLICATE	12/15/2016
Apache Struts contains a flaw related to the parsing of requests. The issue is due to the lack of sanitization of user-supplied parameters that may carry arbitrary OGNL code in a property. With a specially crafted request that is subsequently used as a redirect address, Struts will parse the request and execute the OGNL code.						
95405	MEDIUM	6.8	6.4	8.6	DUPLICATE	12/15/2016
Apache Struts contains a flaw that is triggered when input passed via the 'action:', 'redirect:', and 'redirectAction:' prefixing parameters is not properly sanitized before being used in DefaultActionMapper. This may allow a remote attacker to potentially execute arbitrary code.						
95406	MEDIUM	4.3	2.9	8.6	DUPLICATE	11/10/2015
Apache Struts contains a flaw that allows a remote cross site redirection attack. This flaw exists because the application does not						

validate the 'redirect:' and 'redirectAction:' prefixing parameters upon submission to DefaultActionMapper. This could allow a user to create a specially crafted URL, that if clicked, would redirect a victim from the intended legitimate web site to an arbitrary web site of the attacker's choosing. Such attacks are useful as the crafted URL initially appear to be a web page of a trusted site. This could be leveraged to direct an unsuspecting user to a web page containing attacks that target client side software such as a web browser or document rendering programs.

CVE-2013-1965	HIGH	9.3	10.0	8.6	NEW	07/26/2013

Apache Struts Showcase App 2.0.0 through 2.3.13, as used in Struts 2 before 2.3.14.1, allows remote attackers to execute arbitrary OGNL code via a crafted parameter name that is not properly handled when invoking a redirect.

CVE-2013-1966	HIGH	9.3	10.0	8.6	NEW	07/11/2013

Apache Struts 2 before 2.3.14.1 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag.

CVE-2013-2115	HIGH	9.3	10.0	8.6	NEW	07/11/2013

Apache Struts 2 before 2.3.14.2 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag. NOTE: this issue is due to an incomplete fix for CVE-2013-1966.

CVE-2013-2134	HIGH	9.3	10.0	8.6	NEW	01/06/2017

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted action name that is not properly handled during wildcard matching, a different vulnerability than CVE-2013-2135.

CVE-2013-2135	HIGH	9.3	10.0	8.6	NEW	05/05/2014

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted value that contains both "${}" and "%{}" sequences, which causes the OGNL code to be evaluated twice.

CVE-2013-2248	MEDIUM	5.8	4.9	8.6	NEW	12/30/2016

Multiple open redirect vulnerabilities in Apache Struts 2.0.0 through 2.3.15 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in a parameter using the (1) redirect: or (2) redirectAction: prefix.

CVE-2013-2251	HIGH	9.3	10.0	8.6	NEW	12/07/2016

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.

CVE-2013-4310	MEDIUM	5.8	4.9	8.6	NEW	05/05/2014

Apache Struts 2.0.0 through 2.3.15.1 allows remote attackers to bypass access controls via a crafted action: prefix.

CVE-2013-4316	HIGH	10.0	10.0	10.0	NEW	12/07/2016

Apache Struts 2.0.0 through 2.3.15.1 enables Dynamic Method Invocation by default, which has unknown impact and attack vectors.

CVE-2014-0094	MEDIUM	5.0	2.9	10.0	NEW	01/06/2017

The ParametersInterceptor in Apache Struts before 2.3.16.1 allows remote attackers to "manipulate" the ClassLoader via the class parameter, which is passed to the getClass method.

CVE-2014-0112	HIGH	7.5	6.4	10.0	NEW	01/06/2017

ParametersInterceptor in Apache Struts before 2.3.16.2 does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0094.

CVE-2014-0113	HIGH	7.5	6.4	10.0	NEW	01/06/2017

CookieInterceptor in Apache Struts before 2.3.16.2, when a wildcard cookiesName value is used, does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0094.

CVE-2014-0116	MEDIUM	5.8	4.9	8.6	NEW	04/16/2015

CookieInterceptor in Apache Struts 2.x before 2.3.16.3, when a wildcard cookiesName value is used, does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and modify session state via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0113.

CVE-2014-7809	MEDIUM	6.8	6.4	8.6	NEW	10/25/2016
Apache Struts 2.0.0 through 2.3.x before 2.3.20 uses predictable <s:token/> values, which allows remote attackers to bypass the CSRF protection mechanism.						
CVE-2016-0785	HIGH	10.0	10.0	10.0	NEW	11/28/2016
Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation.						
CVE-2016-2162	MEDIUM	4.3	2.9	8.6	NEW	11/28/2016
Apache Struts 2.x before 2.3.25 does not sanitize text in the Locale object constructed by I18NInterceptor, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors involving language display.						
CVE-2016-3081	HIGH	9.3	10.0	8.6	NEW	11/30/2016
Apache Struts 2.x before 2.3.20.2, 2.3.24.x before 2.3.24.2, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via method: prefix, related to chained expressions.						
CVE-2016-3082	HIGH	10.0	10.0	10.0	NEW	11/28/2016
XSLTResult in Apache Struts 2.x before 2.3.20.2, 2.3.24.x before 2.3.24.2, and 2.3.28.x before 2.3.28.1 allows remote attackers to execute arbitrary code via the stylesheet location parameter.						
CVE-2016-3093	MEDIUM	5.0	2.9	10.0	NEW	11/28/2016
Apache Struts 2.0.0 through 2.3.24.1 does not properly cache method references when used with OGNL before 3.0.12, which allows remote attackers to cause a denial of service (block access to a web site) via unspecified vectors.						
CVE-2016-4003	MEDIUM	4.3	2.9	8.6	NEW	11/28/2016
Cross-site scripting (XSS) vulnerability in the URLDecoder function in JRE before 1.8, as used in Apache Struts 2.x before 2.3.28, when using a single byte page encoding, allows remote attackers to inject arbitrary web script or HTML via multi-byte characters in a url-encoded parameter.						
CVE-2016-4436	HIGH	7.5	6.4	10.0	NEW	10/21/2016
Apache Struts 2 before 2.3.29 and 2.5.x before 2.5.1 allow attackers to have unspecified impact via vectors related to improper action name clean up.						
CVE-2017-5638	HIGH	10.0	10.0	10.0	NEW	03/29/2017
The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.						
103918	HIGH	10.0	10.0	10.0	DUPLICATE	01/12/2017
Apache Commons FileUpload contains flaw that is due to ParametersInterceptor allowing access to the 'class' parameter. This may allow a remote attacker to manipulate the ClassLoader and execute arbitrary Java code.						
93646	MEDIUM	6.8	6.4	8.6	DUPLICATE	12/15/2016
Apache Struts contains a flaw related to the parsing of requests. The issue is due to the lack of sanitization of user-supplied parameters that may carry arbitrary OGNL code in a property. With a specially crafted request that is subsequently used as a redirect address, Struts will parse the request and execute the OGNL code.						
95405	MEDIUM	6.8	6.4	8.6	DUPLICATE	12/15/2016
Apache Struts contains a flaw that is triggered when input passed via the 'action:', 'redirect:', and 'redirectAction:' prefixing parameters is not properly sanitized before being used in DefaultActionMapper. This may allow a remote attacker to potentially execute arbitrary code.						
95406	MEDIUM	4.3	2.9	8.6	DUPLICATE	11/10/2015
Apache Struts contains a flaw that allows a remote cross site redirection attack. This flaw exists because the application does not validate the 'redirect:' and 'redirectAction:' prefixing parameters upon submission to DefaultActionMapper. This could allow a user to create a specially crafted URL, that if clicked, would redirect a victim from the intended legitimate web site to an arbitrary web site of the attacker's choosing. Such attacks are useful as the crafted URL initially appear to be a web page of a trusted site. This could be leveraged to direct an unsuspecting user to a web page containing attacks that target client side software such as a web browser or document rendering programs.						
CVE-2013-1965	HIGH	9.3	10.0	8.6	NEW	07/26/2013

Apache Struts Showcase App 2.0.0 through 2.3.13, as used in Struts 2 before 2.3.14.1, allows remote attackers to execute arbitrary OGNL code via a crafted parameter name that is not properly handled when invoking a redirect.

CVE-2013-1966	HIGH	9.3	10.0	8.6	NEW	07/11/2013

Apache Struts 2 before 2.3.14.1 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag.

CVE-2013-2115	HIGH	9.3	10.0	8.6	NEW	07/11/2013

Apache Struts 2 before 2.3.14.2 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag. NOTE: this issue is due to an incomplete fix for CVE-2013-1966.

CVE-2013-2134	HIGH	9.3	10.0	8.6	NEW	01/06/2017

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted action name that is not properly handled during wildcard matching, a different vulnerability than CVE-2013-2135.

CVE-2013-2135	HIGH	9.3	10.0	8.6	NEW	05/05/2014

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted value that contains both "${}" and "%{}" sequences, which causes the OGNL code to be evaluated twice.

CVE-2013-2248	MEDIUM	5.8	4.9	8.6	REMEDIATION COMPLETE	12/30/2016

Multiple open redirect vulnerabilities in Apache Struts 2.0.0 through 2.3.15 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in a parameter using the (1) redirect: or (2) redirectAction: prefix.

CVE-2013-2251	HIGH	9.3	10.0	8.6	NEW	12/07/2016

Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.

CVE-2013-4310	MEDIUM	5.8	4.9	8.6	NEW	05/05/2014

Apache Struts 2.0.0 through 2.3.15.1 allows remote attackers to bypass access controls via a crafted action: prefix.

CVE-2013-4316	HIGH	10.0	10.0	10.0	NEW	12/07/2016

Apache Struts 2.0.0 through 2.3.15.1 enables Dynamic Method Invocation by default, which has unknown impact and attack vectors.

CVE-2014-0094	MEDIUM	5.0	2.9	10.0	REMEDIATION REQUIRED	01/06/2017

The ParametersInterceptor in Apache Struts before 2.3.16.1 allows remote attackers to "manipulate" the ClassLoader via the class parameter, which is passed to the getClass method.

CVE-2014-0112	HIGH	7.5	6.4	10.0	NEW	01/06/2017

ParametersInterceptor in Apache Struts before 2.3.16.2 does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0094.

CVE-2014-0113	HIGH	7.5	6.4	10.0	MITIGATED	01/06/2017

CookieInterceptor in Apache Struts before 2.3.16.2, when a wildcard cookiesName value is used, does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0094.

CVE-2014-0116	MEDIUM	5.8	4.9	8.6	NEW	04/16/2015

CookieInterceptor in Apache Struts 2.x before 2.3.16.3, when a wildcard cookiesName value is used, does not properly restrict access to the getClass method, which allows remote attackers to "manipulate" the ClassLoader and modify session state via a crafted request. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-0113.

CVE-2014-7809	MEDIUM	6.8	6.4	8.6	REMEDIATION REQUIRED	10/25/2016

Apache Struts 2.0.0 through 2.3.x before 2.3.20 uses predictable <s:token/> values, which allows remote attackers to bypass the CSRF protection mechanism.

CVE-2016-0785	HIGH	10.0	10.0	10.0	NEW	11/28/2016

Apache Struts 2.x before 2.3.28 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation.

CVE-2016-2162	MEDIUM	4.3	2.9	8.6	NEW	11/28/2016

Apache Struts 2.x before 2.3.25 does not sanitize text in the Locale object constructed by I18NInterceptor, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors involving language display.

CVE-2016-3081	HIGH	9.3	10.0	8.6	IGNORED	11/30/2016

Apache Struts 2.x before 2.3.20.2, 2.3.24.x before 2.3.24.2, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via method: prefix, related to chained expressions.

CVE-2016-3082	HIGH	10.0	10.0	10.0	NEW	11/28/2016

XSLTResult in Apache Struts 2.x before 2.3.20.2, 2.3.24.x before 2.3.24.2, and 2.3.28.x before 2.3.28.1 allows remote attackers to execute arbitrary code via the stylesheet location parameter.

CVE-2016-3093	MEDIUM	5.0	2.9	10.0	NEW	11/28/2016

Apache Struts 2.0.0 through 2.3.24.1 does not properly cache method references when used with OGNL before 3.0.12, which allows remote attackers to cause a denial of service (block access to a web site) via unspecified vectors.

CVE-2016-4003	MEDIUM	4.3	2.9	8.6	NEEDS REVIEW	11/28/2016

Cross-site scripting (XSS) vulnerability in the URLDecoder function in JRE before 1.8, as used in Apache Struts 2.x before 2.3.28, when using a single byte page encoding, allows remote attackers to inject arbitrary web script or HTML via multi-byte characters in a url-encoded parameter.

CVE-2016-4436	HIGH	7.5	6.4	10.0	PATCHED	10/21/2016

Apache Struts 2 before 2.3.29 and 2.5.x before 2.5.1 allow attackers to have unspecified impact via vectors related to improper action name clean up.

CVE-2017-5638	HIGH	10.0	10.0	10.0	NEW	03/29/2017

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.

Apache Xalan (Java) 2.7.1

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2014-0107	HIGH	7.5	6.4	10.0	NEW	01/06/2017

The TransformerFactory in Apache Xalan-Java before 2.7.2 does not properly restrict access to certain properties when FEATURE_SECURE_PROCESSING is enabled, which allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources via a crafted (1) xalan:content-header, (2) xalan:entities, (3) xslt:content-header, or (4) xslt:entities property, or a Java property that is bound to the XSLT 1.0 system-property function.

Apache Xerces2 J 2.6.2

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
95418	HIGH	7.1	6.9	8.6	NEW	11/03/2016

Apache Xerces2 Java Parser contains a flaw in the scanPseudoAttribute() function in XMLScanner.java that is triggered when handling XML pseudo attributes. This may allow a remote attacker to cause a denial of service.

Hibernate Validator 4.1.0.Final

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2014-3558	MEDIUM	5.0	2.9	10.0	NEW	03/27/2015

ReflectionHelper (org.hibernate.validator.util.ReflectionHelper) in Hibernate Validator 4.1.0 before 4.2.1, 4.3.x before 4.3.2, and 5.x before 5.1.2 allows attackers to bypass Java Security Manager (JSM) restrictions and execute restricted reflection calls via a

crafted application.

Jersey 1.13

Sun GPL With Classpath Exception v2.0 (reciprocal)
Common Development and Distribution License 1.1 (weak reciprocal)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
103881	MEDIUM	5.0	2.9	10.0	NEW	03/01/2014

Jersey contains a flaw in the bg resource method. The issue is due to the program exposing potentially sensitive information in a WebApplicationException with a MessageException as the excepton message. This may allow a remote attacker to gain access to a list of configured converters and other sensitive information.

Jetty: Java based HTTP, Servlet, SPDY, WebSocket Server 6.0.1

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
36079	LOW	3.5	2.9	6.8	DUPLICATE	11/16/2010

Apache Tomcat contains a flaw that allows a remote cross site scripting attack. This flaw exists because the Manager and Host Manager applications do not validate the filename of files uploaded via the /manager/html/upload utility. This could allow a user to create a specially crafted URL that would execute arbitrary code in a user's browser within the trust relationship between the browser and the server, leading to a loss of integrity.

62054	MEDIUM	4.3	2.9	8.6	DUPLICATE	03/09/2014

Apache Tomcat contains a flaw that allows a remote attacker to traverse outside of a restricted path of the host's work directory. The issue is due to Apache Tomcat not properly sanitizing the contents of a WAR file before it is deployed, which could be exploited by a directory traversal sequence in the file name(s) to delete and possibly create malicious files in the host's work directory.

70809	MEDIUM	5.0	2.9	10.0	DUPLICATE	03/23/2016

Apache Tomcat contains a flaw that may allow a remote denial of service. The issue is triggered when an error occurs due to the 'maxHttpHeaderSize' limit failing to be enforced in the 'NIO HTTP connector', which may be exploited with a crafted web request to cause a denial of service due to an 'OutOfMemory' error.

71557	MEDIUM	4.3	2.9	8.6	DUPLICATE	03/23/2016

The HTML Manager Interface in Apache Tomcat contains multiple flaws that allow a remote cross-site scripting (XSS) attack. This flaw exists because the application does not validate certain unspecified input related to the display-name tag before returning it to the user. This may allow a user to create a specially crafted URL that would execute arbitrary script code in a user's browser within the trust relationship between their browser and the server.

71558	LOW	1.2	2.9	1.9	DUPLICATE	03/23/2016

Apache Tomcat contains a flaw that allows a local attacker to traverse outside of a restricted path. The issue is due to the 'SecurityManager' not properly making the 'ServletContext' attribute read-only, allowing for directory traversal style attacks (e.g., ../../). This directory traversal attack would allow the attacker to manipulate arbitrary files.

87227	MEDIUM	5.0	2.9	10.0	DUPLICATE	03/23/2016

Apache Tomcat contains a flaw that may allow a remote denial of service. The issue is triggered when the parseHeaders() function in InternalNioInputBuffer.java fails to properly verify the permitted size during the parsing of request headers. With a specially crafted header, a remote attacker can cause an OutOfMemoryError exception, which will result in a loss of availability for the program.

88093	MEDIUM	4.3	2.9	8.6	DUPLICATE	03/19/2016

Apache Tomcat contains a flaw that is triggered during the handling of a null session request. This may allow a remote attacker to bypass the CSRF prevention filter.

88094	MEDIUM	4.3	2.9	8.6	DUPLICATE	03/19/2016

Apache Tomcat contains a flaw that is triggered during FORM authentication when handling a request that has been apended with /j_security_check. This may allow a remote attacker to bypass security constraints.

88095	LOW	2.6	2.9	4.9	DUPLICATE	06/30/2014

Apache Tomcat contains a flaw that may allow a remote denial of service. The issue is triggered when an error occurs in the NIO

connector during the handling of a terminated connection, which will result in an infinite loop. This will cause a loss of availability for the program.

CVE-2006-6969	MEDIUM	6.8	6.4	8.6	NEW	03/07/2011

Jetty before 4.2.27, 5.1 before 5.1.12, 6.0 before 6.0.2, and 6.1 before 6.1.0pre3 generates predictable session identifiers using java.util.random, which makes it easier for remote attackers to guess a session identifier through brute force attacks, bypass authentication requirements, and possibly conduct cross-site request forgery attacks.

CVE-2007-0450	MEDIUM	5.0	2.9	10.0	NEW	03/07/2011

Directory traversal vulnerability in Apache HTTP Server and Tomcat 5.x before 5.5.22 and 6.x before 6.0.10, when using certain proxy modules (mod_proxy, mod_rewrite, mod_jk), allows remote attackers to read arbitrary files via a .. (dot dot) sequence with combinations of (1) "/" (slash), (2) "\" (backslash), and (3) URL-encoded backslash (%5C) characters in the URL, which are valid separators in Tomcat but not in Apache.

CVE-2007-1355	MEDIUM	4.3	2.9	8.6	NEW	08/24/2013

Multiple cross-site scripting (XSS) vulnerabilities in the appdev/sample/web/hello.jsp example application in Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.23, and 6.0.0 through 6.0.10 allow remote attackers to inject arbitrary web script or HTML via the test parameter and unspecified vectors.

CVE-2007-2449	MEDIUM	4.3	2.9	8.6	NEW	10/30/2012

Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attackers to inject arbitrary web script or HTML via the portion of the URI after the ';' character, as demonstrated by a URI containing a "snp /snoop.jsp;" sequence.

CVE-2007-2450	LOW	3.5	2.9	6.8	NEW	03/07/2011

Multiple cross-site scripting (XSS) vulnerabilities in the (1) Manager and (2) Host Manager web applications in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote authenticated users to inject arbitrary web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

CVE-2007-3382	MEDIUM	4.3	2.9	8.6	NEW	03/07/2011

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 treats single quotes ("'") as delimiters in cookies, which might cause sensitive information such as session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

CVE-2007-3385	MEDIUM	4.3	2.9	8.6	NEW	04/20/2011

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 does not properly handle the \" character sequence in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks.

CVE-2007-3386	MEDIUM	4.3	2.9	8.6	NEW	03/07/2011

Cross-site scripting (XSS) vulnerability in the Host Manager Servlet for Apache Tomcat 6.0.0 to 6.0.13 and 5.5.0 to 5.5.24 allows remote attackers to inject arbitrary HTML and web script via crafted requests, as demonstrated using the aliases parameter to an html/add action.

CVE-2007-5333	MEDIUM	5.0	2.9	10.0	NEW	03/15/2014

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.

CVE-2007-5342	MEDIUM	6.4	4.9	10.0	NEW	03/15/2014

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.

CVE-2007-6286	MEDIUM	4.3	2.9	8.6	NEW	03/15/2014

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.

CVE-2008-0128	MEDIUM	5.0	2.9	10.0	NEW	03/07/2011

The SingleSignOn Valve (org.apache.catalina.authenticator.SingleSignOn) in Apache Tomcat before 5.5.21 does not set the secure flag for the JSESSIONIDSSO cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.

CVE-2008-1232	MEDIUM	4.3	2.9	8.6	NEW	03/15/2017

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.

CVE-2008-1947	MEDIUM	4.3	2.9	8.6	NEW	03/15/2014

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.

CVE-2008-2370	MEDIUM	5.0	2.9	10.0	NEW	03/15/2014

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.

CVE-2008-2938	MEDIUM	4.3	2.9	8.6	NEW	03/07/2011

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.

CVE-2008-5515	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2009-0033	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2009-0580	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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.

CVE-2009-0781	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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."

CVE-2009-0783	MEDIUM	4.6	6.4	3.9	NEW	08/22/2016

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.

CVE-2009-1523	MEDIUM	5.0	2.9	10.0	NEW	10/22/2012

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.

CVE-2009-1524	MEDIUM	4.3	2.9	8.6	NEW	07/20/2010

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.

CVE-2009-2693	MEDIUM	5.8	4.9	8.6	NEW	08/22/2016

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.

CVE-2009-2696	MEDIUM	4.3	2.9	8.6	NEW	10/27/2016

Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat on Red Hat Enterprise Linux 5, Desktop Workstation 5, and Linux Desktop 5 allows remote attackers to inject arbitrary web script or HTML via the time parameter, related to "invalid HTML." NOTE: this is due to a missing fix for CVE-2009-0781.

CVE-2009-2901	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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.

CVE-2009-2902	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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.

CVE-2009-3548	HIGH	7.5	6.4	10.0	NEW	08/22/2016

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.

CVE-2009-4609	MEDIUM	5.0	2.9	10.0	NEW	08/08/2011

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.

CVE-2009-4610	MEDIUM	4.3	2.9	8.6	NEW	08/08/2011

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/.

CVE-2009-4611	HIGH	7.5	6.4	10.0	NEW	01/14/2010

Mort Bay Jetty 6.x 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.

CVE-2010-1157	LOW	2.6	2.9	4.9	NEW	08/22/2016

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.

CVE-2010-2227	MEDIUM	6.4	4.9	10.0	NEW	03/16/2014

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."

CVE-2010-3718	LOW	1.2	2.9	1.9	NEW	08/22/2016

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.

CVE-2010-4312	MEDIUM	6.4	4.9	10.0	NEW	11/29/2010

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.

CVE-2011-0013	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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.

CVE-2011-0534	MEDIUM	5.0	2.9	10.0	NEW	03/16/2014

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.

CVE-2011-1184	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2011-2204	LOW	1.9	2.9	3.4	NEW	08/22/2016

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.

CVE-2011-2526	MEDIUM	4.4	6.4	3.4	NEW	08/22/2016

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.

CVE-2011-3190	HIGH	7.5	6.4	10.0	NEW	08/22/2016

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.

CVE-2011-4461	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2011-4858	MEDIUM	5.0	2.9	10.0	NEW	03/05/2014

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.

CVE-2011-5062	MEDIUM	5.0	2.9	10.0	NEW	03/16/2014

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.

CVE-2011-5063	MEDIUM	4.3	2.9	8.6	NEW	03/16/2014

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.

CVE-2011-5064	MEDIUM	4.3	2.9	8.6	NEW	03/16/2014

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.

CVE-2012-0022	MEDIUM	5.0	2.9	10.0	NEW	03/05/2014

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.

CVE-2012-2733	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2012-3544	MEDIUM	5.0	2.9	10.0	NEW	12/11/2014

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.

CVE-2012-3546	MEDIUM	4.3	2.9	8.6	NEW	08/22/2016

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.

CVE-2012-4431	MEDIUM	4.3	2.9	8.6	NEW	12/07/2016

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.

CVE-2012-4534	LOW	2.6	2.9	4.9	NEW	08/22/2016

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.

CVE-2012-5568	MEDIUM	5.0	2.9	10.0	NEW	03/07/2013

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.

CVE-2012-5885	MEDIUM	5.0	2.9	10.0	NEW	08/22/2016

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.

CVE-2012-5886	MEDIUM	5.0	2.9	10.0	NEW	08/19/2013

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.

CVE-2012-5887	MEDIUM	5.0	2.9	10.0	NEW	08/19/2013

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.

CVE-2013-2185	HIGH	7.5	6.4	10.0	NEW	11/01/2016

** DISPUTED ** The readObject method in the DiskFileItem class in Apache Tomcat and JBoss Web, as used in Red Hat JBoss Enterprise Application Platform 6.1.0 and Red Hat JBoss Portal 6.0.0, allows remote attackers to write to arbitrary files via a NULL byte in a file name in a serialized instance, a similar issue to CVE-2013-2186. NOTE: this issue is reportedly disputed by the Apache Tomcat team, although Red Hat considers it a vulnerability. The dispute appears to regard whether it is the responsibility of applications to avoid providing untrusted data to be deserialized, or whether this class should inherently protect against this issue.

CVE-2013-4286	MEDIUM	5.8	4.9	8.6	NEW	12/07/2016

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.

CVE-2013-4322	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017

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.

CVE-2013-4444	MEDIUM	6.8	6.4	8.6	NEW	01/06/2017

Unrestricted file upload vulnerability in Apache Tomcat 7.x before 7.0.40, in certain situations involving outdated java.io.File code and a custom JMX configuration, allows remote attackers to execute arbitrary code by uploading and accessing a JSP file.

CVE-2013-4590	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017

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.

CVE-2013-6357	MEDIUM	6.8	6.4	8.6	NEW	11/14/2013

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

CVE-2014-0075	MEDIUM	5.0	2.9	10.0	NEW	01/06/2017

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.

CVE-2014-0096	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017

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.

CVE-2014-0099	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017

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.

CVE-2014-0119	MEDIUM	4.3	2.9	8.6	NEW	01/06/2017

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.

CVE-2014-0227	MEDIUM	6.4	4.9	10.0	NEW	01/02/2017

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.

CVE-2014-0230	HIGH	7.8	6.9	10.0	NEW	12/30/2016

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.

CVE-2014-7810	MEDIUM	5.0	2.9	10.0	NEW	12/30/2016

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.

CVE-2015-5174	MEDIUM	4.0	2.9	8.0	NEW	12/05/2016

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.

CVE-2015-5345	MEDIUM	5.0	2.9	10.0	NEW	12/05/2016

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.

CVE-2016-0706	MEDIUM	4.0	2.9	8.0	NEW	12/05/2016

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.

CVE-2016-0714	MEDIUM	6.5	6.4	8.0	NEW	12/05/2016

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.

CVE-2016-5388	MEDIUM	5.1	6.4	4.9	NEW	02/16/2017

Apache Tomcat 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.

CVE-2016-6816	MEDIUM	6.8	6.4	8.6	NEW	03/24/2017

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.

CVE-2016-8735	HIGH	7.5	6.4	10.0	NEW	04/12/2017

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.

Spring Framework 3.0.0

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
68931	HIGH	7.5	6.4	10.0	DUPLICATE	09/01/2015

Spring Security contains a flaw related to the processing of security constraints. The issue is triggered when a remote attacker adds certain URL path parameters to a request. This may allow the attacker to bypass security constraints.

88154	MEDIUM	5.0	2.9	10.0	DUPLICATE	09/01/2015

VMware SpringSource Spring Security contains a flaw in the DaoAuthenticationProvider. The issue is due to passwords not being properly checked when a user is not found. With a specially crafted series of login requests, a remote attacker can cause the response delay to be shorter and allow valid usernames to be enumerated.

CVE-2010-1622	MEDIUM	6.0	6.4	6.8	NEW	12/06/2016

SpringSource Spring Framework 2.5.x before 2.5.6.SEC02, 2.5.7 before 2.5.7.SR01, and 3.0.x before 3.0.3 allows remote attackers to execute arbitrary code via an HTTP request containing class.classLoader.URLs[0]=jar: followed by a URL of a crafted .jar file.

CVE-2011-2730	HIGH	7.5	6.4	10.0	NEW	01/17/2015

VMware SpringSource Spring Framework before 2.5.6.SEC03, 2.5.7.SR023, and 3.x before 3.0.6, when a container supports Expression Language (EL), evaluates EL expressions in tags twice, which allows remote attackers to obtain sensitive information via a (1) name attribute in a (a) spring:hasBindErrors tag; (2) path attribute in a (b) spring:bind or (c) spring:nestedpath tag; (3) arguments, (4) code, (5) text, (6) var, (7) scope, or (8) message attribute in a (d) spring:message or (e) spring:theme tag; or (9) var, (10) scope, or (11) value attribute in a (f) spring:transform tag, aka "Expression Language Injection."

CVE-2011-2894	MEDIUM	6.8	6.4	8.6	NEW	02/13/2012

Spring Framework 3.0.0 through 3.0.5, Spring Security 3.0.0 through 3.0.5 and 2.0.0 through 2.0.6, and possibly other versions deserialize objects from untrusted sources, which allows remote attackers to bypass intended security restrictions and execute untrusted code by (1) serializing a java.lang.Proxy instance and using InvocationHandler, or (2) accessing internal AOP interfaces, as demonstrated using deserialization of a DefaultListableBeanFactory instance to execute arbitrary commands via the java.lang.Runtime class.

CVE-2013-4152	MEDIUM	6.8	6.4	8.6	NEW	11/28/2016

The Spring OXM wrapper in Spring Framework before 3.2.4 and 4.0.0.M1, when using the JAXB marshaller, does not disable entity resolution, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via an XML external entity declaration in conjunction with an entity reference in a (1) DOMSource, (2) StAXSource, (3) SAXSource, or (4) StreamSource, aka an XML External Entity (XXE) issue.

CVE-2013-6429	MEDIUM	6.8	6.4	8.6	NEW	11/28/2016

The SourceHttpMessageConverter in Spring MVC in Spring Framework before 3.2.5 and 4.0.0.M1 through 4.0.0.RC1 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152 and CVE-2013-7315.

CVE-2013-7315	MEDIUM	6.8	6.4	8.6	NEW	11/28/2016

The Spring MVC in Spring Framework before 3.2.4 and 4.0.0.M1 through 4.0.0.M2 does not disable external entity resolution for the StAX XMLInputFactory, which allows context-dependent attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML with JAXB, aka an XML External Entity (XXE) issue, and a different vulnerability than CVE-2013-4152. NOTE: this issue was SPLIT from CVE-2013-4152 due to different affected versions.

CVE-2014-0054	MEDIUM	6.8	6.4	8.6	NEW	11/28/2016

The Jaxb2RootElementHttpMessageConverter in Spring MVC in Spring Framework before 3.2.8 and 4.0.0 before 4.0.2 does not disable external entity resolution, which allows remote attackers to read arbitrary files, cause a denial of service, and conduct CSRF attacks via crafted XML, aka an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4152, CVE-2013-7315, and CVE-2013-6429.

CVE-2014-1904	MEDIUM	4.3	2.9	8.6	NEW	07/29/2015

Cross-site scripting (XSS) vulnerability in web/servlet/tags/form/FormTag.java in Spring MVC in Spring Framework 3.0.0 before 3.2.8 and 4.0.0 before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via the requested URI in a default action.

Spring Security 3.0.0.RELEASE

Apache License 2.0 (permissive)

Vulnerability Name	Severity	Base	Exploitability	Impact	Status	Published
CVE-2010-3700	MEDIUM	5.0	2.9	10.0	NEW	11/06/2010

VMware SpringSource Spring Security 2.x before 2.0.6 and 3.x before 3.0.4, and Acegi Security 1.0.0 through 1.0.7, as used in IBM WebSphere Application Server (WAS) 6.1 and 7.0, allows remote attackers to bypass security constraints via a path parameter.

CVE-2011-2731	MEDIUM	5.1	6.4	4.9	NEW	10/23/2013

Race condition in the RunAsManager mechanism in VMware SpringSource Spring Security before 2.0.7 and 3.0.x before 3.0.6 stores the Authentication object in the shared security context, which allows attackers to gain privileges via a crafted thread.

CVE-2011-2732	MEDIUM	4.3	2.9	8.6	NEW	12/06/2012

CRLF injection vulnerability in the logout functionality in VMware SpringSource Spring Security before 2.0.7 and 3.0.x before 3.0.6 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the spring-security-redirect parameter.

CVE-2011-2894	MEDIUM	6.8	6.4	8.6	NEW	02/13/2012

Spring Framework 3.0.0 through 3.0.5, Spring Security 3.0.0 through 3.0.5 and 2.0.0 through 2.0.6, and possibly other versions deserialize objects from untrusted sources, which allows remote attackers to bypass intended security restrictions and execute untrusted code by (1) serializing a java.lang.Proxy instance and using InvocationHandler, or (2) accessing internal AOP interfaces, as demonstrated using deserialization of a DefaultListableBeanFactory instance to execute arbitrary commands via the java.lang.Runtime class.

CVE-2012-5055	MEDIUM	5.0	2.9	10.0	NEW	12/28/2012

DaoAuthenticationProvider in VMware SpringSource Spring Security before 2.0.8, 3.0.x before 3.0.8, and 3.1.x before 3.1.3 does not check the password if the user is not found, which makes the response delay shorter and might allow remote attackers to enumerate valid usernames via a series of login requests.

Generated for **HPE Security**
Fortify on Demand

***NOTE**: This report lists **only** the vulnerable components for this Hub project. To view a complete list of Open Source components identified, go to Duck Hub Demo 2.0.*