Adeptia Connect v3.4 third party dependency scanning report

Product : Adeptia Connect v3.4

Tool Used : White Source v20.8.1.2

Date of Scanning : 15th Dec 2020

Library	Severity	Vulnerability Id	CVSS 2	CVSS 3	Vector	Description	Published	Modified	Status	Comment
spring-web-5.2.6.RELEASE.jar	High	CVE-2016-1000027	7.5	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Pivotal Spring Framework 4.1.4 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required.	2020-01-02	2020-01-09	False Positive	This vulnerability is applicable on spring framework v4.1.4. Adeptia Connect v3.3 is using spring framework version v5.2.1. So this vulnerability is not applicable.
jetty-webapp-9.4.32.v20200930.jar	High	CVE-2020-27216	4.6	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0.beta2O, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race then they will have read and write permission to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any code is ever executed out of this temporary directory, this can lead to a local privilege escalation vulnerability.	2020-10-23	2020-12-11	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
batik-transcoder-1.12.jar	High	CVE-2019-17566	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Apache Batik is vulnerable to server-side request forgery, caused by improper input validation by the "xlink:href" attributes. By using a specially-crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests.	2020-11-12	2020-12-11	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
woodstox-core-5.0.3.jar	High	WS-2018-0629	9.1	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H	The woodstox-core package is vulnerable to improper restriction of XXE reference.	2018-08-23	2020-10-28	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.

jackson-databind-2.10.1.jar	High	CVE-2020-25649	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.	2020-12-03	2020-12-11	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
hibernate-core-5.4.22.Final.jar	High	CVE-2020-25638	5.8	7.4	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.	2020-12-02	2020-12-04	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
not-yet-commons-ssl-0.3.9.jar	Medium	CVE-2014-3604	6.8			Certificates.java in Not Yet Commons SSL before 0.3.15 does not properly verify that the server hostname matches a domain name in the	2014-10-25	2018-01-05	Not Planned.	This jar is the dependency of opensaml-2.6.4.jar. So we need to upgrade both.
opensaml-2.6.4.jar	Medium	CVE-2015-1796	4.3			The PKIX trust engines in Shibboleth Identity Provider before 2.4.4 and OpenSAML Java (OpenSAML-J) before 2.6.5 trust candidate X.509 credentials when no trusted names are available for the entityID, which allows remote attackers to impersonate an entity via a certificate issued by a shibmd:KeyAuthority trust anchor.	2015-07-08	2016-11-30	Not Planned	Authentic upgrade version is not available for this jar. So it's upgrade is not planned in this release.
spring-web-5.2.6.RELEASE.jar	Medium	CVE-2020-5421	3.6	6.5	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:N	In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.	2020-09-19	2020-11-20	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
httpclient-4.5.10.jar	Medium	CVE-2020-13956	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the library as java.net.URI object and pick the wrong target host for request execution.	2020-12-02	2020-12-04	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.

jetty-server-9.4.32.v20200930.jar	Medium	CVE-2020-27218	5.8	4.8	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L	In Eclipse Jetty version 9.4.0.RC0 to 9.4.34.v20201102, 10.0.0.alpha0 to 10.0.0.beta2, and 11.0.0.alpha0 to 11.0.0.beta2, if GZIP request body inflation is enabled and requests from different clients are multiplexed onto a single connection, and if an attacker can send a request with a body that is received entirely but not consumed by the application, then a subsequent request on the same connection will see that body prepended to its body. The attacker will not see any data but may inject data into the body of the subsequent request.	2020-11-28	2020-12-11	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
commons-httpclient-3.1.jar	Medium	CVE-2012-5783	5.8			Apache Commons HttpClient 3.x, as used in Amazon Flexible Payments Service (FPS) merchant Java SDK and other products, does not 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 an arbitrary valid certificate.	2012-11-04	2018-01-05	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.
guava-28.1-jre.jar	Low	CVE-2020-8908	2.1	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	A temp directory creation vulnerability exist in Guava versions prior to 30.0 allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava com.google.common.io.Files.createTempDir(). The permissions granted to the directory created default to the standard unix-like /tmp ones, leaving the files open. We recommend updating Guava to version 30.0 or later, or update to Java 7 or later, or to explicitly change the permissions after the creation of the directory if neither are possible.	2020-12-10	2020-12-11	To be planned	Currently this is a candidate of ACE v3.5 (next release) planning list. The confirmation will be given once the planning for v3.5 is completed.