Adeptia Connect v3.3 third party dependency scanning report

Product : Adeptia Connect v3.3
Tool Used : White Source v20.5.1.255
Date of Scanning : 13th July 2020

Library	Severity	Vulnerability Id	CVSS 2	CVSS 3	Vector	Description	Status	Explanation
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.	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.
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 subject's Common Name (CN) field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 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.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
hibernate-validator-6.1.0.Final.jar	Medium	CVE-2020-10693	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
ant-1.8.2.jar	Medium	CVE-2012-2098	5.0			Algorithmic complexity vulnerability in the sorting algorithms in bzip2 compressing stream (BZip2CompressorOutputStream) in Apache Commons Compress before 1.4.1 allows remote attackers to cause a denial of service (CPU consumption) via a file with many repeating inputs.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
ant-1.8.2.jar	Medium	CVE-2020-1945	3.3	6.3	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N	Apache Ant 1.1 to 1.9.14 and 1.10.0 to 1.10.7 uses the default temporary directory identified by the Java system property java.io.tmpdir for several tasks and may thus leak sensitive information. The fixcrlf and replaceregexp tasks also copy files from the temporary directory back into the build tree allowing an attacker to inject modified source files into the build process.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
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.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
mysql-connector-java-8.0.18.jar	Medium	CVE-2020-2934	5.1	5.0	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.19 and prior and 5.1.48 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors.	To be planned	Currently this is a candidate of ACE v3.4 (next release) planning list. The confirmation will be given once the planning for v3.4 is completed.
log4j-core-2.13.1.jar	Low	CVE-2020-9488	4.3	3.7	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.		