ACE_3_5_Dependencies_Scanning_Report

Adeptia Connect v3.5 third party dependency scanning report

Product : Adeptia Connect v3.5

Tool Used : White Source 21.5.1.1.276

Date of Scanning : 27-May-2021

Library	Severity	Vulnerability Id	CVSS 2	CSS 3	Vector	Description	Published	Modified	Status	Comment
spring-web-5.2.9.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 v3.5 is using spring framework version v5.2.1. So this vulnerability is not applicable.
	Medium	CVE-2021-22118	6.5	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.	2021-05-27	2021-05-27	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
jetty-io-9.4.38.v20210224.jar	High	CVE-2021-28165	7.8	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon receiving a large invalid TLS frame.	2021-04-01	2021-05-17	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
json-smart-2.3.jar	High	CVE-2021-27568	6.4	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2021-05-04	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 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 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.	2014-10-25	2018-01-05	To be 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	To be planned	Authentic upgrade version is not available for this jar. So it's upgrade is not planned in this release.

pdfbox-2.0.17.jar	Medium	CVE-2021-27807	4.3	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	A carefully crafted PDF file can trigger an infinite loop while loading the file. This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.	2021-03-19	2021-05-21	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
	Medium	CVE-2021-27906	4.3	5.5	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	A carefully crafted PDF file can trigger an OutOfMemory-Exception while loading the file. This issue affects Apache PDFBox version 2.0.22 and prior 2.0.x versions.	2021-03-19	2021-05-21	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
jetty-webapp-9.4.38.v20210224.jar	Medium	CVE-2021-28164	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	In Eclipse Jetty 9.4.37.v20210219 to 9.4.38.v20210224, the default compliance mode allows requests with URIs that contain %2e or %2e%2e segments to access protected resources within the WEB-INF directory. For example a request to /context/%2e/WEB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	2021-04-01	2021-05-07	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
jetty-server-9.4.38.v20210224.jar	Medium	CVE-2021-28164	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	In Eclipse Jetty 9.4.37.v20210219 to 9.4.38.v20210224, the default compliance mode allows requests with URIs that contain %2e or %2e%2e segments to access protected resources within the WEB-INF directory. For example a request to /context/%2e/WEB-INF/web.xml can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	2021-04-01	2021-05-07	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
spring-security-web-5.3.8.RELEASE.jar	Medium	WS-2016-7107	5.9	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CSRF tokens in Spring Security through 5.4.6 are vulnerable to a breach attack. Spring Security always returns the same CSRF token to the browser.	2016-08-02	2021-04-12	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
commons-io-2.6.jar	Medium	CVE-2021-29425	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.	2021-04-13	2021-05-18	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
commons-io-2.4.jar	Medium	CVE-2021-29425	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.	2021-04-13	2021-05-18	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.

jersey-common-2.29.1.jar	Medium	CVE-2021-28168	2.1	5.5	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users.	2021-04-22	2021-05-07	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.
commons-dbcp2-2.7.0.jar	Low	WS-2020-0287	3.0	3.0	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	Apache commons-dbcp through 2.8.0 exposes sensitive information via JMX. If a BasicDataSource is created with jmxName set, password property is exposed/exported via jmx and is visible for everybody who is connected to jmx port.	2020-03-04	2021-03-28	To be planned	Currently this is a candidate of ACE v3.6 (next release) planning list. The confirmation will be given once the planning for v3.6 is completed.