ACE_3_6_Dependencies_Scanning_Report

Adeptia Connect v3.6 third party dependencies scanning report

Product : Adeptia Connect v3.6

Tool Used : White Source 21.5.1.1.276

Date of Scanning : 14-Dec-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 v3.6 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
commons-compress-1.19.jar	High	CVE-2021-35515	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	2021-07-13	2021-12-02	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	High	CVE-2021-35516	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.	2021-07-13	2021-12-02	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	High	CVE-2021-35517	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	When reading a specially crafted TAR archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' tar package.	2021-07-13	2021-12-02	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.

	High	CVE-2021-36090	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	When reading a specially crafted ZIP archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' zip package.	2021-07-13	2021-11-04	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
xmlsec-2.1.4.jar	High	CVE-2021-40690	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	All versions of Apache Santuario - XML Security for Java prior to 2.2.3 and 2.1.7 are vulnerable to an issue where the "secureValidation" property is not passed correctly when creating a KeyInfo from a KeyInfoReference element. This allows an attacker to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.	2021-09-19	2021-12-03	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
jsoup-1.12.1.jar	High	CVE-2021-37714	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	jsoup is a Java library for working with HTML. Those using jsoup versions prior to 1.14.2 to parse untrusted HTML or XML may be vulnerable to DOS attacks. If the parser is run on user supplied input, an attacker may supply content that causes the parser to get stuck (loop indefinitely until cancelled), to complete more slowly than usual, or to throw an unexpected exception. This effect may support a denial of service attack. The issue is patched in version 1.14.2. There are a few available workarounds. Users may rate limit input parsing, limit the size of inputs based on system resources, and/or implement thread watchdogs to cap and timeout parse runtimes.	2021-08-18	2021-10-20	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
netty-handler-4.1.65.Final.jar	High	WS-2020-0408	7.4	7.4		An issue was found in all versions of io.netty:netty-all. Host verification in Netty is disabled by default. This can lead to MITM attack in which an attacker can forge valid SSL/TLS certificates for a different hostname in order to intercept traffic that doesn’t intend for him. This is an issue because the certificate is not matched with the host.	2020-06-22	2021-08-24	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	High	CVE-2021-37136	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The Bzip2 decompression decoder function doesn't allow setting size restrictions on the decompressed output data (which affects the allocation size used during decompression). All users of Bzip2Decoder are affected. The malicious input can trigger an OOME and so a DoS attack	2021-10-19	2021-12-03	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	High	CVE-2021-37137	5.0	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	The Snappy frame decoder function doesn't restrict the chunk length which may lead to excessive memory usage. Beside this it also may buffer reserved skippable chunks until the whole chunk was received which may lead to excessive memory usage as well. This vulnerability can be triggered by supplying malicious input that decompresses to a very big size (via a network stream or a file) or by sending a huge skippable chunk.	2021-10-19	2021-12-03	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	Medium	CVE-2021-34429	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	For Eclipse Jetty versions 9.4.37-9.4.42, 10.0.1-10.0.5 & 11.0.1-11.0.5, URIs can be crafted using some encoded characters to access the content of the WEB-INF directory and/or bypass some security constraints. This is a variation of the vulnerability reported in CVE-2021-28164/GHSA-v7ff-8wcx-gmc5.	2021-07-15	2021-12-02	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
jetty-server-9.4.38.v20210224.jar jetty-servlets-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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
	Medium	CVE-2021-28169	5.0	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, it is possible for requests to the ConcatServlet with a doubly encoded path to access protected resources within the WEB-INF directory. For example a request to `/concat?/%2557EB-INF/web.xml` can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.	2021-06-09	2021-12-10	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
kafka-clients-2.8.0.jar	Medium	CVE-2021-38153	4.3	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Some components in Apache Kafka use `Arrays.equals` to validate a password or key, which is vulnerable to timing attacks that make brute force attacks for such credentials more likely to be successful. Users should upgrade to 2.8.1 or higher, or 3.0.0 or higher where this vulnerability has been fixed. The affected versions include Apache Kafka 2.0.0, 2.0.1, 2.1.0, 2.1.1, 2.2.0, 2.2.1, 2.2.2, 2.3.0, 2.3.1, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.6.2, 2.7.0, 2.7.1, and 2.8.0.	2021-05-20	2021-06-22	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
spring-core-5.2.9.jar spring-core-5.3.9.jar spring-webmvc-5.2.9.RELEASE.jar	Medium	CVE-2021-22096	4.0	4.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.	2021-10-28	2021-11-29	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
netty-codec-http-4.1.65.Final.jar	Medium	CVE-2021-43797	6.5	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N	Netty prior to version 4.1.7.1.Final skips control chars when they are present at the beginning / end of the header name. It should instead fail fast as these are not allowed by the spec and could lead to HTTP request smuggling. Failing to do the validation might cause netty to "sanitize" header names before it forward these to another remote system when used as proxy. This remote system can't see the invalid usage anymore, and therefore does not do the validation itself. Users should upgrade to version 4.1.7.1.Final to receive a patch.	2021-12-09	2021-12-09	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
bcprov-jdk15on-1.64.ja	Medium	CVE-2020-15522	4.3	5.9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.	2021-05-20	2021-06-22	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.

tomcat-embed-core-9.0.45.jar	Medium	CVE-2021-33037	5.0	5.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	2021-07-12	2021-12-02	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.
antisamy-1.5.8.jar	Medium	CVE-2021-35043	4.3	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	OWASP AntiSamy before 1.6.4 allows XSS via HTML attributes when using the HTML output serializer (XHTML is not affected). This was demonstrated by a javascript: URL with &#00058 as the replacement for the : character.	2021-07-19	2021-12-01	To be planned	Currently this is a candidate of ACE v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 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 v3.7 (next release) planning list. The confirmation will be given once the planning for v3.7 is completed.