Third party libraries known CVE issues

Delft-FEWS uses third party libraries and analyses these libraries using the OWASP dependency check tool. See https://owasp.org/www-project-dependency-check/

Common Vulnerabilities and Exposures (CVE) with CVE score Critical and High

This page keeps track of known CVE issues in libraries that are distributed with Delft-FEWS and the upgrade strategy of these libraries. The Common Vulnerability Scoring System (CVSS) of severity Critical and High are reported here.

date	CVE	library	description	versions	Risk for Delft-FEWS	JIRA	upgrade strategy
February 2024	CVE-2002-0059	zlib1.dll	The decompression algorithm in zlib 1.1.3 and earlier, as used in many different utilities and packages, causes inflateEnd to release certain memory more than once (a "double free"), which may allow local and remote attackers to execute arbitrary code via a block of malformed compression data. FEWS uses a more recent version (1.2.13 - 1.3.1) but apparently the OWASP dependency checker is not able to detect this, therefore we consider this a false alarm.	2022.02 - current	False positive	FEWS-27692 - Jira project doesn't exist or you don't have permission to view it.	False positive, no action required

December 2023	CVE-2022-46337	`derby-10.16.1.1.jar`	A cleverly devised username might bypass LDAP authentication checks. In LDAP-authenticated Derby installations, this could let an attacker fill up the disk by creating junk Derby databases. In LDAP-authenticated Derby installations, this could also allow the attacker to execute malware which was visible to and executable by the account which booted the Derby server. FEWS only uses embedded Derby in local Standalone-installations, embedded Derby does not support LDAP and is not accessible over a network in such configurations. Therefore this warning can safely be discarded as a false positive.	2021.02 - current	False positive	⚠ FEWS-30391 - Jira project doesn't exist or you don't have permission to view it.	False positive, no action required
November 2023	CVE-2023-36052	azure-core-*.jar azure-identity-*.jar	Azure CLI REST Command Information Disclosure Vulnerability The Microsoft Security Response Center (MSRC) was made aware of a vulnerability where Azure Command-Line Interface (CLI) could expose sensitive information, including credentials, through GitHub Actions logs. The researcher, from Palo Alto Networks Prisma Cloud, found that Azure CLI commands could be used to show sensitive data and output to Continuous Integration and Continuous Deployment (CI/CD) logs. Microsoft recommends that customers update to the latest version of Azure CLI (2.54) and follow the guidance provided below to help prevent inadvertently exposing secrets through CI/CD logs. A notification in the Azure Portal was sent to customers who recently used Azure CLI commands informing them of an available update.	2032.02 - current	This is a very specific use case where the role these Java libraries could play is not clear. FEWS is not using this library in the context of a CLI or Github actions so this OWASP alert is considered a false positive.		False positive, no action required

⚠ FEW S-30379 - Jira project doesn't exist or you don't have permission to view it.

						⚠ FEWS-30236 - Jira project doesn't exist or you don't have permission to view it.	

November 2023	**CVE-2023-36415**	azure-identity-*.jar	Azure Identity SDK Remote Code Execution Vulnerability *Above is the only information supplied* For the current 1.11.0 version we consider this a false alert for a vulnerability that needs to be addressed in the .net based Azure SDK. so it will be suppressed, specifically for CVE-2023-36415	2021.02 - current	False positive	 FEWS-30236 - Jira project doesn't exist or you don't have permission to view it.	

October 2023	**CVE-2023-45853**	zlib1.dll libz.so.1.2.13	MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. The main author, Mark Adler states (github): Minizip is not part of zlib. The source code is provided in the contrib directory of the zlib distribution, along with several other such contributions, as a courtesy. This is not a zlib vulnerability. Additionally, zlib.def has been checked to verify that at least the windows version contains no minizip methods.	2022.02 - current	False positive	⚠ FEW S-27692 - Jira proje ct does n't exist or you don't have per miss ion to view it.	False positive, no action required.

October 2023	**CVE-2023-4586**	netty-transport-4.1.91.Final.jar netty-all-4.1.79.Final.jar	A vulnerability was found in the Hot Rod client provided by the Netty library. This security issue occurs as the Hot Rod client does not enable hostname validation when using TLS, possibly resulting in a man-in-the-middle (MITM) attack. Netty is used by FEWS in the context of Microsoft Azure (AzureIotHub import) and THREDDS which is used by the archive server. Hot Rod is a very specific TCP client server protocol used by the Jboss Infinispan product. There is no indication of any kind that the Hot Rod protocol is used by FEWS or THREDDS in any way so this is considered a false positive warning.	2020.02 - current	False positive	 FEWS-26050 - Jira project doesn't exist or you don't have permission to view it.	False positive. No action required.

September 2023	**CVE-2023-34040**	spring-boot-3.0.7.jar	In Spring for Apache Kafka 3.0.9 and earlier and versions 2.9.10 and earlier, a possible deserialization attack vector existed, but only if unusual configuration was applied. An attacker would have to construct a malicious serialized object in one of the deserialization exception record headers. Specifically, an application is vulnerable when all of the following are true: - The user does not configure an ErrorHandlingDeserializer for the key and/or value of the record - The user explicitly sets container properties checkDeserExWhenKeyNull and /or checkDeserExWhenValueNull container properties to true. - The user allows untrusted sources to publish to a Kafka topic By default, these properties are false, and the container only attempts to deserialize the headers if an ErrorHandlingDeserializer is configured. The ErrorHandlingDeserializer prevents the vulnerability by removing any such malicious headers before processing the record. Two out of three conditions mentioned in the description are not met in the case of FEWS. This library is currently only used for the admin interface, which should never be made available for use by "untrusted sources" over the internet.	2020.02 - 2023.01	False positive	⚠ FEWS-29191 - Jira project doesn't exist or you don't have permission to view it.	False positive. No action required.

Februari 2023	**CVE-2023-25158**	gt-26.4.jar gt-20.0.jar net.opengis.fes-20.0.jar	The GeoTools implementation of the OpenGIS Filter Encoding Standard (FES) has been found to contain SQL Injection Vulnerabilities when executing OGC Filters with JDBCDataStore implementations. Delft-FEWS has no such JDBCDataStore implementation and the Filter functionality has been included only to support a client side implementation of the OpenGIS WFS interface. FEWS only uses this to implement OpenGIS WFS viewing capability, no server side WFS or FES implementation that could be prone to SQL injection exists in FEWS.	2019-02 - 2022.02	False positive	 FEWS-27037 - Jira project doesn't exist or you don't have permission to view it.	False positive. No action required.

December 2022	**CVE-2016-4432**	qpid-jms-client-0.51.0-p.jar	The AMQP 0-8, 0-9, 0-91, and 0-10 connection handling in Apache Qpid Java before 6.0.3 might allow remote attackers to bypass authentication and consequently perform actions via vectors related to connection state logging. Delft-FEWS only uses the client, not the AMQP server.	2021.01 - current	False Positive.	 FEWS-28377 - Jira project doesn't exist or you don't have permission to view it.	False positive. No action required. Jar file can be removed from bin folder if the Azure IOT Hub import is not used. See also AzureIot Hub
Feb 2023 August 2022	**CVE-2022-31197**	postgresql-42.4.1.jar postgresql-42.3.3.jar	PG 42.3.3 was flagged in Aug 2022. PG 42.4.1 was flagged only since Feb 2023. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection.	2022.01 - 2022.02	False Positive. PgResultSet#refreshRow() is not used		False positive. 2022.02 and 2023.01 have been upgraded to 42.5.3.

⚠ FEWS-28737 - Jira project doesn't exist or you don't have permission to view it.

						⚠ FEWS-27632 - Jira project doesn't exist or you don't have permission to view it.	

May 2022	**CVE-2016-1000027**	spring-core-5.3.19.jar	The spring framework allows to use a http invoker that uses object serialization that may be vulnerable for Remote Code Execution. https://docs.spring.io/spring-framework/docs/current/reference/html/integration.html#remoting-httpinvoker.	2022.01 - 2019.02	Only used in Admin interface where the described scenario is not used.	 FEWS-27230 - Jira project doesn't exist or you don't have permission to view it.	False positive. The HTTP Invoker method that is vulnerable is not used in any of the Delft-FEWS components. Upgrading won't help either since it won't be removed from the library. It has been marked as deprecated and will be removed in spring 6.

Mar 2022	**CVE-2022-26336**	poi-scratchpad 5.2	A shortcoming in the HMEF package of poi-scratchpad (Apache POI) allows an attacker to cause an Out of Memory exception. This package is used to read TNEF files (Microsoft Outlook and Microsoft Exchange Server). If an application uses poi-scratchpad to parse TNEF files and the application allows untrusted users to supply them, then a carefully crafted file can cause an Out of Memory exception. This issue affects poi-scratchpad version 5.2.0 and prior versions. Users are recommended to upgrade to poi-scratchpad 5.2.1.	2021.02 only	False positive. FEWS uses some of the Apache POI library (for the interval statistics dialog) but not the scratchpad, which is in a separate jar file.	 FEWS-26865 - Jira project doesn't exist or you don't have permission to view it.	False positive. Upgrade in development to latest release.

Feb 2022	**CVE-2022-21724**	postgresql-42.2.22.jar	A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade.	2021.02 - 2022.01	PG jdbc database url manipulation enables code execution loaded via arbitrary classes.	 FEWS-26908 - Jira project doesn't exist or you don't have permission to view it.	Upgrade to postgresql-42.3.3.jar

Nov 2021	**CVE-2021-43466**	thymeleaf-3.0.12.RELEASE.jar	In the thymeleaf-spring5:3.0.12 component, thymeleaf combined with specific scenarios in template injection may lead to remote code execution. Comment of Thymeleaf developer: I'd like to explain that CVE-2021-43466 only affects those applications that contain controllers or controller configurations that take a request parameter and directly use it, without previous filtering, as the name of the view to be rendered		Only used in Admin interface where the described scenario is not used.	 FEW S-26228 - Jira proje ct does n't exist or you don't have per miss ion to view it.	False positive. No action required. Once version 3.0.13 is available we can upgrade the jar to avoid this false alarm.

Oct 2021 Jan 2022	**CVE-2021-42340**, **CVE-2022-23181**	tomcat-embed-core-9.0.50.jar	The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError. The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.	2021.02 - 2022.02	False positives. Delft-FEWS web applications don't use web sockets and doesn't use session persistence with the FileStorage.	 FEWS-26049 - Jira project doesn't exist or you don't have permission to view it.	False positives Upgrade in development only to latest tomcat 9 release.

Oct 2021	**CVE-2021-37136**, **CVE-2021-37137**	netty-all-4.1.48.Final.jar	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. and 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.		False alarm. Bzip decoder is not used. Excessive memory usage might lead to a failing FSS in the worst case. Since the Azure IOT Hub is quite well secured, the risk is limited.	 FEW S-26050 - Jira proje ct does n't exist or you don't have per miss ion to view it.	False positive. Upgrade in development to latest release.

Jun 2021	**CVE-2021-33813**	jdom-2.02.jar	An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request.		Might be used in imports that use opendap. But since the library is not used in a service component, the risk is limited.	 FEWS-25545 - Jira project doesn't exist or you don't have permission to view it.	Dependency of ucar netcdf libraries. JDOM library has been upgraded to: jdom2-2.0.6.1.jar since 2022.01.

Mar 2019	**CVE-2019-7611**	elasticsearch-core-6.4.3.jar	A permission issue was found in Elasticsearch versions before 5.6.15 and 6.6.1 when Field Level Security and Document Level Security are disabled and the _aliases, _shrink, or _split endpoints are used		Elastic search as distributed as part of the archive server and doesn't have Field Level or Document Level Seurity disabled. As long as the provided settings are not changed, there is no risk.	 FEW S-25543 - Jira proje ct does n't exist or you don't have per miss ion to view it.	False positive. No need to upgrade since the archive server configuration is correct. Once a fix is available we can upgrade the jar to avoid this false alarm.

May 2018	CVE-2018-1258	spring-security-core-5.4.8.jar, spring-security-oauth2-core-5.4.8.jar	Spring Framework version 5.0.5 when used in combination with any versions of Spring Security contains an authorization bypass when using method security. An unauthorized malicious user can gain unauthorized access to methods that should be restricted. CWE-863 Incorrect Authorization		False alarm. Spring security is used in the Admin Interface, but doesn't use version 5.0.5 of the spring framework, but a higher version.	⚠ FEWS-25865 - Jira project doesn't exist or you don't have permission to view it.	False positive. No action required. Once a fix is available we can upgrade the jar to avoid this false alarm.

Commonly distributed 3rd party executables with CVE score Critical and High

date	CVE	library	description	versions	Risk for Delft-FEWS	JIRA	upgrade strategy
Apr 2022	CVE-2022-28085	htmldoc (optionally supplied component not part of the Delft-FEWS binaries)	A flaw was found in htmldoc commit 31f7804. A heap buffer overflow in the function pdf_write_names in ps-pdf.cxx may lead to arbitrary code execution and Denial of Service (DoS).	Up to 2022-03-24	**Up to (excluding) 2022-03-24**	FEWS-27693	When using htmldoc, the end-user must be supplied with updated version from https://github.com/michaelrsweet/htmldoc/releases

Deltares Open Archive common vulnerabilities and exposures (CVE) with CVE score Critical and High

This page keeps track of known CVE issues in libraries that are distributed with the Deltares Open Archive and the upgrade strategy of these libraries. The Common Vulnerability Scoring System (CVSS) of severity Critical and High are reported here.

THREDDS

date	CVE	description	versions	Risk for Deltares Open Archive	JIRA	upgrade strategy

August 2023	**CVE-2023-39017**	quartz-jobs 2.3.2 and below was discovered to contain a code injection vulnerability in the component org.quartz.jobs.ee.jms.SendQueueMessageJob.execute. This vulnerability is exploited via passing an unchecked argument. This is a indirect dependency as this library is used by the THREDDS data service which is part of the archive. The source code of the current 4.6 THREDDS release has been checked to make sure that this does not use the SendQueueMessageJob class in any way so it is considered a false positive within the context of FEWS.	up to current	False positive. THREDDS does not use this part of the quartz library.	⚠ FEWS-29689 - Jira project doesn't exist or you don't have permission to view it.	
July 2023	**CVE-2023-2976**	Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.	up to current	False positive. User has to already have access to server.	FEWS-29496	Fix available when Thredds 5.5 stable is released.

March 2023	**CVE-2023-20860**	Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.	up to current	False positive. Spring security is not used.	⚠ FEWS-29336 - Jira project doesn't exist or you don't have permission to view it.	
October 2021	**CVE-2020-13936**	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container	up to current	False positive. Users in THREDDS are not allowed to upload velocity templates.	FEWS-29325	
november 2018	**CVE-2018-1258**	Spring Framework version 5.0.5 when used in combination with any versions of Spring Security contains an authorization bypass when using method security. An unauthorized malicious user can gain unauthorized access to methods that should be restricted.	up to current	False positive. Spring security is not used.	FEWS-29331,FEWS-29332, FEWS-29334 and FEWS-29335	
February 2020	**CVE-2016-1000027**	Pivotal Spring Framework through 5.3.16 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. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.	up to current	False positive. Java is not used for deserialization.	FEWS-29336	
December 2022	**CVE-2022-3510**	A parsing issue similar to CVE-2022-3171, but with Message-Type Extensions in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	up to current	False positive. Parsing is internally handled by THREDDS.	FEWS-29337	

November 2022	CVE-2022-3171	A parsing issue with binary data in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	up to current	False positive. Parsing is internally handled by THREDDS.	FEWS-29337	
December 2022	CVE-2022-45688	A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.	up to current	False positive. XML to json is not used in THREDDS.	FEWS-29342	
October 2023	CVE-2023-5072	Denial of Service in JSON-Java versions up to and including 20230618. A bug in the parser means that an input string of modest size can lead to indefinite amounts of memory being used.	up to current	False positive, the archive is always protected by a proxy which does not allow untrusted inputs	FEWS-29342	
July 2023	CVE-2023-38286	Thymeleaf through 3.1.1.RELEASE, as used in spring-boot-admin (aka Spring Boot Admin) through 3.1.1 and other products, allows sandbox bypass via crafted HTML. This may be relevant for SSTI (Server Side Template Injection) and code execution in spring-boot-admin if MailNotifier is enabled and there is write access to environment variables via the UI.	up to current	False positive, THREDDS does not use MailNotifier	FEWS-29646	
June 2021	CVE-2021-33813	An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request.	up to current	False positve. THREDDS is not vulnerable for this type of attack.	FEWS-29346	

Opensearch

date	CVE	description	versions	Risk for Deltares Open Archive	JIRA	upgrade strategy
january 2020	CVE-2019-20444	HttpObjectDecoder.java in Netty before 4.1.44 allows an HTTP header that lacks a colon, which might be interpreted as a separate header with an incorrect syntax, or might be interpreted as an "invalid fold."	up to 202301	202301 and higher have a fix which checks that headers have a colon. If not the request is rejected	FEWS-29351	
december 20222	CVE-2022-3064	Parsing malicious or large YAML documents can consume excessive amounts of CPU or memory.	up to 202301	False positive. The only yaml file used is the yaml file for the config. This file is only accessible by admins.	FEWS-29357	

Deltares archive server

date	CVE	description	versions	Risk for Deltares Open Archive	JIRA	upgrade strategy
April 2022	CVE-2022-24785	Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.	up to 202301	False positive. User provided local strings are not used.	FEWS-29358	

June 2022	CVE-2022-31129	moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment were found to use an inefficient parsing algorithm. Specifically using string-to-date parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific inputs. Users may notice a noticeable slowdown is observed with inputs above 10k characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re)DoS attacks. The problem is patched in 2.29.4, the patch can be applied to all affected versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths accepted from user input.	up to 202301	False positive. User cannot pass user defined string for date parsing.	FEWS-29358	
June 2022	CVE-2020-7746	chartjs.js is a JavaScript library which is included with primefaces 8.0 jar file and triggers a warning for this vulnerability. As the Archive Web UI is not using chartjs functionality this is considered a false positive and thers is no need to update primefaces in 2021.02 and older branches.	up to 2021.02	False positive, the archive web interface does not use this functionality.	FEWS-24730	

Apache Tomcat CVE score Critical and High

date	CVE	description	versions	Risk for Delft-FEWS	JIRA	upgrade strategy
November 2023	**CVE-2023-456589**	Tomcat did not correctly parse HTTP trailer headers. A specially crafted trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.	• 10.1.0 - 10.1.15 • 9.0.0 - 9.0.82			Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.
October 2023	**CVE-2023-42795**	When recycling various internal objects, including the request and the response, prior to re-use by the next request/response, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next.	• 10.1.0 - 10.1.13 • 9.0.0 - 9.0.80			Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.

October 2023	**CVE-2023-44487**	Tomcat's HTTP/2 implementation was vulnerable to the rapid reset attack. The denial of service typically manifested as an OutOfMemoryError.	• 10.1.0 - 10.1.13 • 9.0.0 - 9.0.80			Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.
October 2023	**CVE-2023-45648**	Tomcat did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.	• 10.1.0 - 10.1.13 • 9.0.0 - 9.0.80			Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.
June 2023	**CVE-2023-34981**	A regression in the fix for bug 66512 in Apache Tomcat 11.0.0-M5, 10.1.8, 9.0.74 and 8.5.88 meant that, if a response did not include any HTTP headers no AJP SEND_HEADERS messare woudl be sent for the response which in turn meant that at least one AJP proxy (mod_proxy_ajp) would use the response headers from the previous request leading to an information leak.	• Apache Tomcat 10.1.8 • Apache Tomcat 9.0.74	None, we do not use AJP proxy		Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.
May 2023	**CVE-2022-28079**	The fix for CVE-2023-24998 was incomplete. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.	• Apache Tomcat 10.1.5 to 10.1.7 • Apache Tomcat 9.0.71 to 9.0.73			Upgrade to latest version of Apache Tomcat. Note: Delft-FEWS releases < 2023.01 require Apache Tomcat 9, release >= 2023.01 require Apache Tomcat 10.