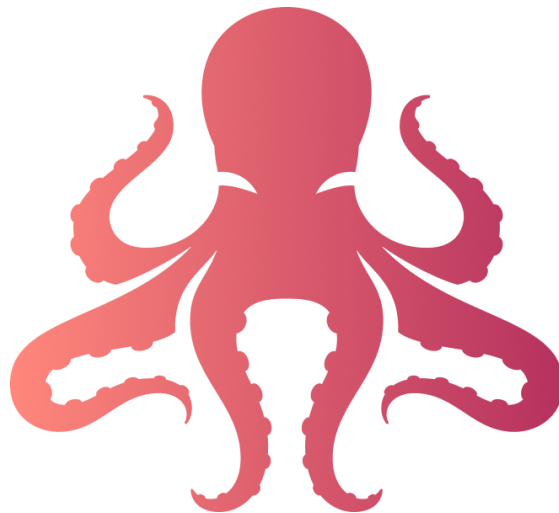


Waratek Java Upgrade

Version 22.0.5

2023-09-28

Release Notes



Overview

This release introduces support for Elasticsearch version 8.x and also includes some minor bug fixes.

Supported Environments

Management Console

- 5.2.0+

Portal Dedicated

- 6.4.2

Oracle HotSpot Java 1.4 32-bit (HotSpot 8 host)

- Linux
- Windows Server

Oracle HotSpot Java 1.4 32-bit (HotSpot 7 host)

- Solaris SPARC

Oracle HotSpot Java 4 64-bit (HotSpot 8 / 11 host)

- Solaris SPARCv9 only

Oracle HotSpot Java 5, 6, 7 32-bit (HotSpot 7 host)

- Solaris SPARC

Oracle HotSpot Java 5, 6, 7, 8 for 32-bit: (HotSpot / Corretto / OpenJDK 8 host)

- Linux
- Windows Server

Oracle HotSpot Java 5, 6, 7, 8 for 64-bit: (HotSpot / Corretto / OpenJDK 8 or 11 host)

- Linux
- Windows Server

IBM J9 Java 6, 7, 8 32-bit and 64-bit (J9 Java 8 host)

- Linux
- Windows Server
- AIX PPC and PPC64

New Features / Improvements

- PM-527 / W4J-672 Support for Elasticsearch v8 added

Features Which Break Backward Compatibility

- None

Feature Removals

- None

Bug Fixes

- W4J-669 Fix for log messages of supported Armr versions.
- W4J-671 Rules reloading fix for Windows
- W4J-675 Fix for UnsatisfiedLinkError with JBoss EAP on Java8 OpenJDK
- W4J-714 Fix for UnsatisfiedLinkError with awt.Toolkit.initIDs on Java 8 guest 8u381

Known Issues

Common to Java Secure and Upgrade

- REM-2743 JBoss EAP 7.2 On Java Secure with Java 11
- REM-2508 CEF log not reporting if a method declared in a patch cannot be found
- REM-2445 Inconsistent warning messages logged when user inadvertently omits `-Dcom.waratek.log.file` property depending on whether `log.mode` is `LOCAL` or is `BOTH`
- REM-2434 For Java Upgrade, JBoss AS 7.1 and JBoss EAP 6.x running with IBM J9 are unsupported
- REM-2422 When running JRockit 6 with Dynatrace, neither JBoss AS 7.1 nor JBoss EAP 6.x are supported by Java Secure
- REM-1855 `IOException` is unexpectedly thrown when the Deserial rule is absent in certain cases

Java Upgrade Specific

- REM-2642 TLSUpgrade incompatible for apps running legacy SSL libraries such as Oracle Wallet
- ES-1168 / REM-2612 OpenJDK 8u222 guest throws `java.lang.UnsatisfiedLinkError: 'boolean sun.security.ec.ECKeyPairGenerator.native$40864_isCurveSupported(byte[])'`
- REM-2466 AppServers JBoss / Tomcat `java.lang.InternalError: System initialization error`
- REM-2340 In Java Upgrade, the Java 8 JDK option `-Xcheck:jni` is not supported
- REM-2325 For Java Upgrade, JBoss AS 7.1 with AppDynamics when the host is Java 11 is unsupported

22.0.4

New Features / Improvements

- None

Features Which Break Backward Compatibility

- None

Feature Removals

- None

Bug Fixes

- ES-1654 / REM-3212 JLP no longer checks the content of `container_home`

22.0.3

New Features / Improvements

Common to Java Secure & Upgrade

- ES-1422 / PM-330 / PLAT-519 Add Elasticsearch support to the agent Relay
- SECU-303 Empty (null) values and CEF keys are no longer included in the security log message

Java Secure

- PLAT-530 Extend support for Jython running with Waratek Secure

Features Which Break Backward Compatibility

- None

Feature Removals

- None

Bug Fixes

Common to Java Secure and Upgrade

- ES-1490 / REM-2925 `NoClassDefFoundError` when processing HTTP requests for older versions of Weblogic and Oracle EBS
- REM-2927 Allow action not supported with input validation security configuration for validating the HTTP method type
- REM-2928 Parameters to the action directive of ARMR rules, that are unsupported, do not fail validation as expected
- ES-1422 / REM-2929 Unnecessary warning is displayed when the `ElasticsearchRelay` flag is used
- ES-1422 / REM-2930 Agent no longer prints a warning when using ES Relay and Custom Trust Store

- REM-2931 Loading a rules file that contains just comments or whitespace generates a parsing error
- ES-1448 / REM-2932 `com.waratek.AllowSQLiPayloads` does not allow commas to be part of the specified payload
- REM-2933 `methodName` CEF extension is incorrect for deserialization attacks using `ProcessBuilder.start()`
- REM-2934 Timestamp in the security log file was subject to JVM Locale configuration
- ES-1465 / REM-2936 Sanitization rule prevents legit file upload due to XSS detection
- ES-1466 / REM-2937 Process forking rule does not log events properly when there are spaces in file paths
- ES-1457 / REM-2940 `weblogic.servlet.internal.ServletOutputStreamImpl` exhibits `ClassCastException` in Oracle EBS when XSS and CSRF security features are enabled
- REM-2943 Issue with `weblogic/servlet/internal/ServletRequestImpl` class in computing `StackMapFrames` when `BuiltInSelfTest` for recompiler are enabled
- REM-2947 `NoClassDefFoundError` when processing HTTP requests for older versions of WebLogic and Oracle EBS
- REM-2948 Agent was unable to retransform the bytecode after Java Flight Recorder transformation
- REM-2950 `StringUtilsTest.splitWithCommaDelimiter` class failing due to incorrect assertion

Java Secure Specific

- ES-1444 / REM-2926 `BuiltInSelfTest` failures: `StackOverflow` during taint propagation for URL encoding
- REM-2935 Early Oracle HotSpot Java 8 releases contain a fatal bug that is incompatible with Waratek agents. Waratek agents will skip such JVMs by default
- REM-2938 Early check of multipart-formdata parameter values
- REM-2939 Process forking is not detected by ARMR process rule when command contains arguments
- REM-2941 Calling the method `java/sql/XML.getString()` will result in an `IllegalArgumentException` when `BuiltInSelfTest` is enabled
- ES-1444 / REM-2942 Fixed circular references during sanitization inspection.
- REM-2944 ARMR sanitization log entry contains CEF extensions that have a value of null

Java Upgrade Specific

- REM-2945 ARMR sanitization rule does not trigger on Upgrade for malicious input in `ServletInputStream.readLineTests`
- REM-2946 `BuiltInSelfTest` reporting NSL illegal host object in AWT handles
- REM-2973 IBM JVM class error when running with latest Java 8 J9

22.0.1

New Features / Improvements

- None

Features Which Break Backward Compatibility

- None

Feature Removals

- None

Bug Fixes

Common to Java Secure and Upgrade

- ES-1428 / REM-2815 Issue with network rules when no logging is configured

22.0.0

New Features / Improvements

Common to Java Secure & Upgrade

- BAR-391 As XML based configuration, eg, for logging, is deprecated and will be removed in a future release, made the changeover easier by including those Java properties in the waratek.properties template
- PM-280 / BAR-416 Bring more clarity to waratek.properties by updating property comments, grouping related properties together and similar
- SPLAT-331 Support for overriding ARMR mods with a version declaration
- SECU-250 / SECU-268 / SECU-269 / SECU-282 / SECU-288 Support new ARMR Data Sanitization rule
- SECU-241 Add HTTP request metadata to Deserial log events
- SPLAT-351 Include the stacktrace in security event log file (for use with the MC). Supported on most ARMR rules, except for: PATCH, SANITIZATION, HTTP-Authenticate, HTTP-Response-Header-Injection.
- SPLAT-346 Support selective reload of modified rules
- SPLAT-333 Security threshold is a lifecycle event related to Waratek Java properties `com.waratek.MaxEventsPerRule=<N>` and `com.waratek.MaxEventsDelay=<seconds>`. When the above limit is reached the additional security event is generated, which is now no longer considered by the MC as an important event
- SPLAT-322 / SPLAT-324 / SPLAT-326 Exclude Waratek Agent from it's own security policy. In three cases accidental application of the wildcard broke Waratek agent functionality which is no longer the case:
 - Using DNS rule could disable DNS lookup of the Management Console and ElasticSearch servers
 - Using Filesystem rule could disable access to the rules file and security log file

- Using Network rule could disable communication to the Management Console and ElasticSearch servers
- SPLAT-315 Ensure consistent logging of tainted data
- PM-262 / SECU-273 New Waratek Java property
`com.waratek.log.cef.redaction=<comma-separated-list>` allows for certain CEF extensions to be omitted. The value is a comma separated list of extensions that will NEVER be included in the event.
- PM-48 / SECU-158 Log the full command line in Process rule
- PM-200 / PLAT-488 Make agent messages more consistent

Specific to Java Upgrade

- PM-271 / PLAT-500 Improvements to the Java Launcher Pack's (JLP) launcher.cfg property comments

Features Which Break Backward Compatibility

Common to Java Secure & Upgrade

- SPLAT-321 Rearrange Load/Link lifecycle events for consistency. Load events occur when an ARMR rule is syntactically valid and all of its parameters are supported and validated against the ARMR app declared version. Link events are logged when an ARMR rule is blended with the Waratek agent, thus, the rule will trigger Execute events if conditions configured for the rule are satisfied.
 - Re-organizing Load and Link events has an impact as to what messages were previously labelled as Load are now Link and vice versa
- SPLAT-314 Split ArmrSocket's CEF `dst` extension
 - Split `dst` CEF extension used for ArmrSocket rules logging into ``local`/`remote`` IP address and `local / remote` port CEF extensions
 - Anything relying on the `dst` extension must be updated
- SPLAT-307 Break metadata of Servlet Header into multiple separate CEF extension
 - A cleanup within the CEF extensions used in security events produced by the agent
 - JSON encoded extension of metadata was removed
 - Introduced number of dedicated extensions: `httpRequestUri`, `httpSessionId`, `httpRemoteUser`, `httpCookies` etc - all of which are documented on a per rule basis
- SPLAT-203 Ensure all security rules log in CEF format only. This affects the following which were non-CEF in previous releases:
 - ARMR rule parsing errors
 - Network Accept rule
 - Native Library rule

Java Upgrade Specific

- None

Feature Removals

Common to Java Secure & Upgrade

- SPLAT-347 Support has been removed for the rules file VERSION header
 - The VERSION header must no longer be present
 - If the VERSION header is present, a `mismatched input` syntax error is thrown

Java Upgrade Specific

- None

Bug Fixes

Common to Java Secure and Upgrade

- REM-2744 Waratek should not start with CSRF rule with collon when there is no port specified like `hosts: ["1.1.1.1:"]`. The agent was silently accepting a typo in the CSRF Same Origin rule configuration of a host name that ended with ":"
- ES-1318 / REM-2730 Hide Waratek classes from classpaths
- REM-2723 Some CEF extension names used in security logging include the dash '-' character but should not
- ES-1167 / ES-1303 / REM-2671 Issue when target file path contains multiple dots in the filename and file extension wildcard is used in ARMR filesystem rules
- ES-1198 / REM-2651 Running certain versions of Tomcat 8 or Tomcat 9 with Java 8 on Windows causes some applications to break when XSS
- ES-1174 / ES-1194 / ES-1279 / REM-2631 `OutOfMemoryException` thrown when tainting is enabled and `StringBuilder` and `StringBuffer` instances expand `String` capacity
- REM-2538 CSRF same-origin hosts whitelisting unexpectedly occurs in some cases when Origin header value does not match host specified in ARMR rule
- REM-2537 Header name missing from log entry if custom message specified in header addition rule
- REM-2536 Header Addition ARMR rule does not accept boolean as a header value
- REM-2516 CSRF hosts whitelisting does not match when host specified in ARMR rule contains uppercase characters
- REM-2489 Wildcarded DNS rule in Protect mode blocks events going to Management Console unless its IP is whitelisted
- REM-2441 CSRF not supported on some versions of IBM J9 Java 8
- REM-2430 Path traversal security log format is incorrect
- REM-2420 Log messages for loading ARMR App error are not accurate
- REM-2412 Deserial rule causes invalid log entries for `System.getenv()`
- REM-2410 Deserial rule causes invalid log entries for `SecurityManager` in `latestUserDefinedLoader` method
- ES-1216 / REM-2400 ARMR SQLi rule fails to load if database vendor of type `any` is specified and both failed and successful injection types
- ES-822 / ES-835 / REM-2370 XSS rule stops Oracle SOA from rendering some pages
- REM-2200 Spiracle web application pages returning 404 when path traversal rule enabled
- REM-2118 Internal Waratek warning displayed - `replicode.core.jaf.InvalidRulesConfigurationException` visible on console when invalid value used with `com.waratek.rules.dir`
- REM-725 Duplicate startup log messages when reloading rules file using autoreload flag

Java Upgrade Specific

- REM-2733 JNA 1.9 source test-case failing with `UnsupportedOperationException` when using Corretto 15 as the host
- REM-2696 WebSphere 8 failing on Upgrade with IBM J9 Java 6 when executing `runConfigActions.bat`

- REM-2624 Fix warning: `com.waratek.AllocUTF16Strings` is not supported; unknown field '`private boolean java.lang.String.hashIsZero`'
- ES-765 / REM-1719 Race condition defining Annotation types in `AnnotationClassLoader`
- REM-1698 Memory leak caused by bad caching of `java.lang.reflection.Method` parameter annotations
- REM-1091 Spring v4.1.x Jasper reports failing on Solaris on Java 8 with `NullPointerException`
- ES-349 / REM-1089 Windows cipher connection issue
- REM-1028 Session rule should regenerate the session ID only if the request is not malicious
- REM-636 Spring 3.2.x: `JdbcTemplateTests` failing with `InvalidUseOfMatchersException` due to mocking issue

19.2.0

New Features / Improvements

- SPLAT-203 Security log messages migrated to the CEF format
- SPLAT-298 The `metadata` CEF extension value, logged by rules that depend on the tainting engine, followed a JSON format. The key value pairs within this JSON object have since been moved to their own separate CEF extensions, avoiding the JSON format altogether
- SPLAT-306 Add Agent name extension to CEF messages in every log entry
- SPLAT-312 CEF extension `port` was replaced by `localPort` and `remotePort`. This gives more context as to what condition the rule event triggers
- SPLAT-313 CEF extension `path` is now logged as part of Path Traversal security events

Backward Incompatibilities / Feature Removals

- SPLAT-203 Security log messages have been migrated to the CEF format
- SPLAT-298 CEF extension `metadata` has been removed and new CEF extensions have been added
- SPLAT-312 CEF extension `port` is replaced by `localPort` and `remotePort`

Bug Fixes

Platform

- REM-2588 The method `createNewFile` of `java.io.File` class should be throwing an `IOException` in the case of a security attack
- ES-1157 / REM-2596 Relative file paths for `com.waratek.log.properties` and `com.waratek.debug.log` properties are not resolved
- REM-2563 `java.lang.UnsatisfiedLinkError` when launching Jenkins v1.614 webapp on WebLogic v10.3.6 and JBossAS v7.1
- ES-1128 REM-2553 `java.lang.UnsupportedOperationException`: The JVM does not support this operation for target encountered under certain conditions
- REM-2459 Fixed incorrect HTTP request rejection when the HTTP verb is `null`

- REM-2438 Security event message in CEF format now contains CEF extensions: `redirectLocation`, `localIpAddress`, `localName`, `serverName`. This specifically impact events from the Open Redirect security feature
- REM-2436 Improved validation message when incorrect log mode is provided
- REM-2431 Java Secure - Elasticsearch 6.5.3 fails with `AccessControlException` `access denied agent core.jar - read`
- ES-1116 / REM-2514 Java Upgrade - Windows, load `freetype.dll` before `fontmanager.dll`
- REM-2590 Java Upgrade - Tomcat fails with `UnsatisfiedLinkError: sun.awt.color.CMM.cmmInit()` while starting up on early updates of Java 6 guests
- ES-1141 / REM-2429 Dynatrace stats not displayed on dashboard
- REM-2090 Incorrect output when auto-onboarding to an application in MC 4.x and higher which has no policy / rules

Security

- REM-2423 Java Upgrade - Network rule's `TcpToSsl` is broken

19.1.0

New Features / Improvements

Platform related:

- SECU-264 New `waratek` flag to manually feed the HTTP session cookie name for configuring CSRF protection using the same origin approach
- PM-230 / SPLAT-300 New `waratek` flags to place counter/limit for security events generation
- PM-232 / AG-245 Implementation for new flag to covering situation where Management Console is not available (`ControllerUnavailableAction.RETRY`)
- AG-246 Removal of Rules 1.0 attributes from the Security Event Request Message

Security related:

- SPLAT-215 Rule loading/outcome messages converted to CEF

Backward Incompatibilities / Feature Removals

- None

Bug Fixes

- REM-2502 Better error feedback on non supported IPv6 addresses in ARMR DNS rule linking
- REM-2488 Incorrect naming of the Waratek Upgrade agent leaking into CEF log messages
- REM-2484 Some security events are no longer treated as ARMR engine life-cycle events
- REM-2481 Removal of `DeserialMaxRead` setting in Waratek Upgrade
- REM-2462 WebSphere ND fails to start on Upgrade (Windows only) when JLP is used
- REM-2436 Improved validation message when incorrect Log Mode is provided
- REM-2354 Log output for ARMR patch rule displays incorrect ARMR version number
- REM-2133 Autoreload feature unloads previous ARMR policies even if the new policy does not have any supported rules to load

- AG-243 Secure/Upgrade connection to Management Console is generating duplicate status checks

19.0.0

New Features / Improvements

Platform related:

- Support for MC 4.4.0
- Add support for FQDN of hostname present in Syslog format headers and CEF extensions
- Allow agent name may be set using new flag `-Dcom.waratek.agent.name=<name>`
- Syslog format is now enforced in security logging output streams
- Automate deployment of Secure and Upgrade
- Productise internal trial feature for Java Secure
- Add flag based configuration for security logging
- Waratek properties file split into read only `waratek.properties` and editable `instance.waratek.properties`
- Support Java 5 on Java Secure
- Initial support for Java 14 hosts for Java Upgrade
- Make all Java Upgrade release artefacts environment agnostic including natives, JLP and config template thus having a single release artefact for all supported environments
- Standardised Java Secure / Upgrade release formats
- Location of security log file, if given by relative path, should resolve to absolute location based on XML file location
- Allow `waratek.properties` to be shared with 2 or more Java agent instances
- For environments where HTTPS configuration of the Agent is difficult, use an external process for secure communication (Http2Https relay)
- Support Java properties as a better means to configure security logging
- The summary message for rules load event or absence of rules is now in the CEF format
- Improve log messaging for when it is necessary to skip the loading of inappropriate patches
- Support the enabling of ARMR patches for specific operating systems
- Add the application's domain to the log message of the Open Redirect rule's security event
- Improve NSLR encoding support when calling JNI RegisterNatives method
- Create a deployment script for Java Secure and Java Upgrade

Security related:

- Protect against:
 - XML Deserial attacks
 - XML Payloads
 - HTTP Response Splitting
 - HTTP Verb Tampering
- Support SQL Injection protection for PostgreSQL
- Allow protection for complete SQL statements to be skipped
- Improve redirect rule for subdomains
- Rename the `SQL` rule type to `SQLi`
- The database vendor will now be present in SQL Injection log messages
- Whitelist specific Deserial privileges
- Whitelist specific SQLi payloads

- Optimize Socket backend on Network rule to improve performance

Backward Incompatibilities / Feature Removals

- Classlink and Reflect rules
- Max Deserial limit
- Heartbeat rule
- Waratek system property `-Dcom.waratek.rootdir=DIRECTORY_PREFIX`
- Storage of files under dirs (Java Upgrade):
 - `/var/lib`
 - `/var/run`
 - `/var/log`
- Each item on the feature removal list constitutes a backward incompatibility if in use
- Release 19.0.0 is not compatible with MC 2.x
- The prefix which precedes every logging entry message has changed (Syslog format)
- Location of security log file, when provided using relative paths, will be resolved based on location of XML log config
- Breaks the original rules reload and absence log format
- Security log messages have been migrated to the CEF format
- The format of a particular log message has changed with `"outcome=failure"` being removed
- Waratek properties split into read only `waratek.properties` and editable `instance.waratek.properties`
- Locations of existing files such as the natives executables have changed in the release artefact