Actifio Report Manager 10.0.4 Release Notes

Copyright, Trademarks, and other Legal Matter

Contents

1 Introduction

About Actifio Report Manager

The Actifio Report Manager (RM) is a web-based reporting service that aggregates data from your VDP appliances (Sky, CDX, and CDS). It is an independent component that runs in its own virtual machine. With it, you can run, schedule, and customize reports about your Actifio environment.

The ActifioNOW Customer Portal

You can always find the latest documentation for RM releases on the ActifioNOW customer portal. From the ActifioNow customer portal you can access the Actifio product documentation, including release notes, and search the knowledge base for answers to specific questions. During the configuration and initialization of your Actifio appliance your Actifio representative provided you with a user name and password for the ActifioNOW customer portal.

To log into the ActifioNOW customer portal:

1. Go to: https://now.actifio.com.
2. When prompted, enter the user name and password provided by your Actifio representative.
3. From the ActifioNOW customer portal you can access:
    - **Product Documentation** - View the user documentation for your Actifio products and releases.
    - **Knowledge Base** - Search across all of the available content for relevant articles.

Product Documentation

- ***Actifio Report Manager Online Help***. Provides information on how to use your Actifio Report Manager.
- ***Actifio Report Manager Deployment Guide***. This guide provides the step-by-step instructions on how to install and upgrade the Actifio Report Manager. It also explains the configuration procedure.
- ***Actifio Report Manager - Schema Definitions PostgreSQL DB***. Describes the database table definitions that Actifio Report Manager uses to store records.
- ***AGM Install and Upgrade Guide***. Provides Actifio Report Manager installation information in AGM.

Actifio Support and Service

Access these locations for help with your Actifio product suite:

Customer Support Numbers	**U.S. Toll-Free Number**: 1.855.392.6810 **From Anywhere**: +1.315.261.7501 **Australia**: 0011 800-16165656 **Germany**: 00 800-16165656 **New Zealand**: 00 800-16165656 **UK**: 0 800-0155019
Customer Support Email	support@actifio.com
Customer Support Portal	http://support.actifio.com/ When prompted, enter the user name and password provided by your Actifio representative.
General Information	http://www.actifio.com

2 Actifio Report Manager 10.0.4 Release Notes

This section describes the new features and enhancements, resolved issues, and upgrade paths of Actifio Report Manager 10.0.4 Release Notes.

Contents

New in This Release

There are no new features added in this release, and this release primarily focuses on improvements and bug fixes.

Compatibility with VDP Appliance Releases

This release only supports VDP appliance 8.0 and above on Sky and CDS appliances. Older releases may continue to function as before, but their use is no longer supported.

Compatibility with VDP Appliance releases

VDP Appliance Release	Basic Compatibility with RM 10.0.4	Reporting on OnVault Pool Consumption	Reporting on SAP HANA	Reporting on External Snapshot Pools	Real-time Reports
Prior to 8.0.0	Unsupported	No	No	No	No
8.0.0 - 8.1.2	Yes	No	No	No	No
8.1.3 - 8.1.4	Yes	Yes	No	No	No
8.1.5 and above	Yes	Yes	Yes	No	No
9.0.1 to 9.0.5	Yes	Yes	Yes	Yes	No
9.0.6 and above	Yes	Yes	Yes	Yes	Yes

Compatibility with VDP Appliance releases

VDP Appliance Release	Basic Compatibility with RM 10.0.4	Reporting on OnVault Pool Consumption	Reporting on SAP HANA	Reporting on External Snapshot Pools	Real-time Reports
10.0.0 and above	Yes	Yes	Yes	Yes	Yes

Upgrade Paths

This section details upgrade paths for this release. This is an optional upgrade.

Software Upgrade of RM 9.0.4 Systems or newer

Existing systems running Report Manager 9.0.4 or newer can upgrade directly to 10.0.4.

Software Upgrade from RM 7.1.3 through RM 9.0.4

Existing systems running Report Manager 7.1.3 must upgrade to RM 9.0.4. From that version, they can upgrade to Report Manager 10.0.4.

Software Upgrade of RM 6.2.x prior to RM 7.1.3

Existing systems running Report Manager 6.2.x must upgrade to Report Manager 7.1.3. From that version, they can upgrade to Report Manager 9.0.4. From there, they can upgrade to Report Manager 10.0.4.

Deprecated Reports

After upgrading the Report Manager from any of the previous versions to Actifio Report Manager 10.0.4, delete if any unused and deprecated reports from the repository.

Deprecated Reports

Folder	Report Name	Deprecated as of
SLA Compliance	SLA Violation Summary For Last 24 Hours	10.0.1
Jobs	Recovery Job Summary	9.0.0
Summary	Application Protection Coverage and Protection Policies	8.0.0
Utilization	Snapshot Pool Utilization History by Application	8.0.0
Utilization	Disk Pool Utilization History	8.0.0
Utilization	Enterprise Managed Data License Consumption	8.0.0
Utilization	Managed Data License Consumptions	8.0.0
Utilization	Managed Data License Consumption History	8.0.0
Protection	Protection Operations Performance History by Day	7.1.0
Protection	Protection Operations Performance History by Operation	7.1.0

Deprecated Reports

Folder	Report Name	Deprecated as of
Protection	Protection Ratio for Selected Appliance	7.1.0
Protection	Protection Ration by SLA for Selected Appliance	7.1.0
Summary	Application Protection Status	7.1.0
Utilization	Daily Snapshot Pool Utilization Summary	7.1.0
Utilization	Top-N Applications Using Dedup Storage	7.1.0
Utilization	Application Consumption to Cumulative vDisk Usage	7.1.0
Utilization	Dedup Pool Utilization History by Application	7.1.0
SLA Compliance	Application Protection Panel	7.0.0
SLA Compliance	Application Protection Panel 15 Days	7.0.0
SLA Compliance	SLA Compliance Statistics by SLA For Last 24 Hours Factor	7.0.0
SLA Compliance	SLA Compliance Summary and Details	7.0.0
SLA Compliance	SLA Compliance Summary and Details by SLA	7.0.0

Resolved Issues

The following table lists the functionality and usability fixes in Actifio Report Manager version 10.0.4.

Issue	Fix	Tracking
The Resource Consumption by Application report does not include unprotected applications.	This issue is now fixed by making the required changes to include unprotected application information.	89187
Schedules are not working after upgrade if it has RM long FQDN name.	This issue is now fixed by changing the column length to VARCHAR.	91396
All the existing custom reports and schedules are deleted while upgrading from 10.0.1 to 10.0.2.	This issue is now fixed by updating the password fields to VARCHAR and removing the character limits.	90047
PostgreSQL shuts down while creating an index on the audit table.	This issue is now fixed by addressing the index-level memory issues.	90011

3 Actifio Report Manager 10.0.2 Release Notes

This section describes the new features and enhancements, resolved issues, and upgrade paths of Actifio Report Manager 10.0.2 Release Notes.

Contents

New in This Release

The following are the list of new features and enhancements added in this release:

Real-time Reporting

Actifio Report Manager (RM) administrators can now run real-time reports. Unlike the built-in reports, which look at cached data that is synchronized from the Actifio appliances on a regular schedule, these reports run directly on the Actifio appliances in real-time. The output from each appliance is then combined in the Report Manager to a single spreadsheet or web page.

An extensive list of these real-time reports is available in the RM user interface. Because these have access to data that is not in the RM data cache, these reports often provide information not available elsewhere. These reports can be scheduled and their output can be emailed, saved in the RM repository, or both.

Details on using real-time reporting can be found in the Online help.

Other Enhancements

- A new Cloud Resource Consumption by Day report is added to show resource consumption of snapshot cloud instances.
- Application type names are standardized to match those used in AGM.
- Job reports now show the target OnVault pool to support multiple OnVault targets in a single policy template.
- Job reports now show jobs that copy logs to OnVault.
- The Daily Protection Status report now has its output grouped by policy template instead of by appliance. There are no more empty sections. This leads to a much more efficient use of the report's real state.
- Reporting has been added for additional database types: SAP HANA, SAP IQ, SAP ASE, SAP MaxDB, IBM Db2, PostgreSQL, MySQL, and MariaDB.
- A filter has been added to the Unresolved Failures report to allow hiding applications whose scheduler is disabled.

Compatibility with VDP Appliance Releases

This release only supports VDP appliance 8.0 and above on Sky and CDS appliances. Older releases may to continue to function as before, but their use is no longer supported.

Compatibility with VDP Appliance releases

VDP Appliance Release	Basic Compatibility with RM 10.0.2	Reporting on OnVault Pool Consumption	Reporting on SAP HANA	Reporting on External Snapshot Pools	Real-time Reports
Prior to 8.0.0	Unsupported	No	No	No	No
8.0.0 - 8.1.2	Yes	No	No	No	No
8.1.3 - 8.1.4	Yes	Yes	No	No	No
8.1.5 and above	Yes	Yes	Yes	No	No
9.0.1 to 9.0.5	Yes	Yes	Yes	Yes	No
9.0.6 and above	Yes	Yes	Yes	Yes	Yes
10.0.0 and above	Yes	Yes	Yes	Yes	Yes

Upgrade Paths

This section details upgrade paths for this release. This is an optional upgrade.

Software Upgrade of RM 9.0.4 Systems or newer

Existing systems running Report Manager 9.0.4 or newer can upgrade directly to 10.0.2.

Software Upgrade from RM 7.1.3 through RM 9.0.4

Existing systems running Report Manager 7.1.3 must upgrade to RM 9.0.4. From that version, they can upgrade to Report Manager 10.0.2.

Software Upgrade of RM 6.2.x prior to RM 7.1.3

Existing systems running Report Manager 6.2.x must upgrade to Report Manager 7.1.3. From that version, they can upgrade to Report Manager 9.0.4. From there, they can upgrade to Report Manager 10.0.2.

Deprecated Reports

After upgrading the Report Manager from any of the previous versions to Actifio Report Manager 10.0.2, delete the unused and deprecated reports from the repository.

Deprecated Reports

Folder	Report Name	Deprecated as of
SLA Compliance	SLA Violation Summary For Last 24 Hours	10.0.1
Jobs	Recovery Job Summary	9.0.0

Deprecated Reports

Folder	Report Name	Deprecated as of
Summary	Application Protection Coverage and Protection Policies	8.0.0
Utilization	Snapshot Pool Utilization History by Application	8.0.0
Utilization	Disk Pool Utilization History	8.0.0
Utilization	Enterprise Managed Data License Consumption	8.0.0
Utilization	Managed Data License Consumptions	8.0.0
Utilization	Managed Data License Consumption History	8.0.0
Protection	Protection Operations Performance History by Day	7.1.0
Protection	Protection Operations Performance History by Operation	7.1.0
Protection	Protection Ratio for Selected Appliance	7.1.0
Protection	Protection Ration by SLA for Selected Appliance	7.1.0
Summary	Application Protection Status	7.1.0
Utilization	Daily Snapshot Pool Utilization Summary	7.1.0
Utilization	Top-N Applications Using Dedup Storage	7.1.0
Utilization	Application Consumption to Cumulative vDisk Usage	7.1.0
Utilization	Dedup Pool Utilization History by Application	7.1.0
SLA Compliance	Application Protection Panel	7.0.0
SLA Compliance	Application Protection Panel 15 Days	7.0.0
SLA Compliance	SLA Compliance Statistics by SLA For Last 24 Hours Factor	7.0.0
SLA Compliance	SLA Compliance Summary and Details	7.0.0
SLA Compliance	SLA Compliance Summary and Details by SLA	7.0.0

Resolved Issues

The following table lists the functionality and usability fixes in Actifio Report Manager version 10.0.2.

Issue	Fix	Tracking
The Application Growth report shows incorrect values for OnVault consumption.	This issue has been fixed.	87051
The Resource Consumption report loads the data very slowly in large environments.	This issue has been fixed.	74916
Reports exported to CSV or Excel formats are truncating header text that is not visible.	This issue has been fixed.	87173

4 Actifio Report Manager 10.0.1 Release Notes

This section describes the new features and enhancements, resolved issues, and upgrade paths of Actifio Report Manager 10.0.1 Release Notes.

Contents

New in This Release

The following are the list of new features and enhancements added in this release:

- User can now login to RM from AGM using single sign-on.
- New reports added in this release:
    - Application Growth
    - Database Log Backup Summary
- The emails generated by scheduled reports can now include the DNS name for Report Manager instead of just the IP address.
- When email configurations are changed or updated, you don't need to restart the Tomcat server.
- The Audit Trail Report by Appliance now supports filtering audit records by user name, audit details, and privileged or unprivileged commands.
- System state recovery jobs are now included in the Recovery Job Details and Recovery Job Summary reports.
- The Restorable Images report now shows the mounted host name.
- Report Manager now supports storing the database partition on LVM to simplify growing the partition if it fills up.
- The Recovery Job Details report now supports running jobs.
- The Resource Consumption reports support OnVault consumption.
- Now you can filter multiple patterns of host and application names using the boolean 'OR' between the search criteria.
- The reporting engine is upgraded to a new version.
- OnVault replication jobs are now included in the Backup Job details and Unresolved Failures reports.
- Added support for SAP HANA, Db2, MySQL, and SAP MaxDB databases.
- The Running Jobs report now supports recovery jobs.
- The Running Jobs report now added with "% Slower Than Previous Durations" filter, where users can create an exception-only report for jobs that are slower than their historic averages.

- The Summary table available in Backup Job Details now includes data copied and a totals row.
- The Unresolved Failures report now tells you when the last successful job occurred for a given application and job type.
- The Snapshot Pool Consumption and Dedup Pool Consumption reports now show consumption details in GB rather than TB.
- See the Resolved Issues section for bug fixes.

Resolved Issues

The following table lists the functionality and usability fixes in Actifio Report Manager version 10.0.1.

Issue	Fix	Tracking
Resource Consumption by Organization report does not show data when the current day is selected.	This issue has been fixed.	77571
In the integrated version, Actifio Report Manager (RM) will sync appliance IP from Actifio Global Manager (AGM) even though the same IP already exists in RM.	This issue has been fixed.	77284
In the integrated version, logical groups added to an organization in AGM does not include its members in RM's organization.	This issue has been fixed.	82560
Failed Jobs report does not show re-provision job types.	This issue has been fixed.	65620
Schedule reports do not show data properly when the email schedule timezone is different from the Report Manager timezone.	This issue has been fixed.	80136
Daily Protection reports do not show StreamSnap jobs when its schedule settings are not inherited from the Snapshot policy.	This issue has been fixed.	79296

5 Known Issues and Limitations

This section describes the known issues and limitations in the Actifio Report Manager 10.0.4 release. It includes the following topics:

- Known Issues in RM 10.0.4 on page 13
- Limitations on page 14

Known Issues in RM 10.0.4

The following table lists the known issues in RM 10.0.4:

Known Issues

Issue	Workaround	Tracking
Actifio Report Manager does not work properly if your browser is configured with an ad-blocking extension (uBlock).	Disable/delete the browser extensions.	25857
Daily Protection Status report has some issues with horizontal scrolling in HTML view.	No known workaround. Issue will be fixed in a future release.	27713
Tool-tip and drill-down functionality in line charts does not work properly when the default zoom level (100%) is changed.	No known workaround. Issue will be fixed in a future release.	27933
When a report is scheduled with a different timezone other than the RM system timezone, it shows incorrect values for Start Time and End Time in the scheduled Report.	No known workaround. Issue will be fixed in a future release. This is a third-party issue: JS-32957.	31889
User cannot apply column filter to show rows which do not have any information.	No known workaround. Issue will be fixed in a future release.	52034
For Job History Summary by Application Report, the totals will count DB+log backups as two jobs (a log backup and a snapshot) even though there is just one job record.	No known workaround. Issue will be fixed in a future release.	53938
Actifio Report Manager shows incorrect system time when upgraded to a 10.x version from 9.x versions.	Root access is required to change the system time, contact Actifio Support.	91404

Known Issues

Issue	Workaround	Tracking
Changes made to saved options do not affect existing scheduled jobs.	Create a new schedule.	62791
The application details section of the Snapshot Pool Consumption report does not include external snapshot pool data.	No known workaround. Issue will be fixed in a future release.	62958
Schedules created on standalone Report Manager by superuser fail to run after migrating to integrated version.	Recreate the schedules on the integrated version.	81518
The header text disappears from every page after page 1 when the column header is to set filter or sort order.	No known workaround. Issue will be fixed in a future release.	86376

Limitations

The following are the limitations Actifio Report Manager 10.0.4:

- PDF report download fails with Google Chrome browser.

  Workaround: Use Save as PDF option in print menu or use an another browser to download the PDF.
- If an external user (VDP appliance users) does not have any applications associated or there is no data available for the selected criteria, the SLA Violation Summary report is not displayed. [RM-133]

  This is a known third-party issue with dual pie-charts. [third-party case no.00065485]

6 Security and Vulnerability Issues

This section lists security and vulnerability fixes for common names for vulnerabilities and exposures (CVEs) resolved as of this release. It includes the following topics:

- Security and Vulnerability Fixes in RM 10.0.4 on page 15
- CVEs Fixed in RM 10.0.4 on page 15
- Known CVE Issues in RM 10.0.4 on page 17

Security and Vulnerability Fixes in RM 10.0.4

The following table lists the Security Vulnerabilities fixed in Actifio Report Manager version 10.0.4:

Tracking Number	Description
There are no Security Vulnerability fixes in Actifio Report Manager version 10.0.4.	

CVEs Fixed in RM 10.0.4

The following table lists the Common Vulnerabilities and Exposures (CVEs) fixed in RM 10.0.4:

Resolved CVEs

Description	CVE
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.	CVE-2021-29425
Apache Batik is vulnerable to server-side request forgery caused by improper input validation by the “xlink:href” attributes. By using a specially crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests.	CVE-2019-17566
A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.	CVE-2020-25649

Resolved CVEs

Description	CVE
A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.	CVE-2020-8908
It was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39, and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.	CVE-2020-17527
Apache Groovy provides extension methods to aid with creating temporary directories. Prior to this fix, Groovy's implementation of those extension methods was using a now superseded Java JDK method call that is potentially not secure on some operating systems in some contexts. Users not using the extension methods mentioned in the advisory are not affected but may wish to read the advisory for further details.	CVE-2020-17521
The XML parsers used by XMLBeans up to version 2.6.0 did not set the properties needed to protect the user from malicious XML input. Vulnerabilities include possibilities for XML Entity Expansion attacks. It affects XMLBeans up to and including v2.6.0.	CVE-2021-23926
Netty is an open-source, asynchronous event-driven network application framework for the rapid development of maintainable high-performance protocol servers & clients. In Netty before version 4.1.59.Final there is a vulnerability on Unix-like systems involving an insecure temp file. When netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method "File.createTempFile" on unix-like systems creates a random file, but, by default will create this file with the permissions "-rw-r--r--". Thus, if sensitive information is written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59.Final. As a workaround, one may specify your own "java.io.tmpdir" when you start the JVM or use "DefaultHttpDataFactory.setBaseDir(...)" to set the directory to something that is only readable by the current user.	CVE-2021-21290
Specific versions of the Java driver that support client-side field level encryption (CSFLE) fail to perform correct hostname verification on the KMS server's certificate. This vulnerability in combination with a privileged network position active MITM attack, could result in interception of traffic between the Java driver and the KMS service rendering Field Level Encryption ineffective. This issue was discovered during internal testing and affects all versions of the Java driver that support CSFLE. The Java async, Scala, and reactive streams drivers are not impacted. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services originating from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don't use Field Level Encryption.	CVE-2021-20328
The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.	CVE-2021-25329

Resolved CVEs

Description	CVE
Apache XmlGraphics Commons 2.4 is vulnerable to server-side request forgery caused by improper input validation by the XMPParser. By using a specially-crafted argument, an attacker could exploit this vulnerability to cause the underlying server to make arbitrary GET requests.	CVE-2020-11988
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.	CVE-2021-27568
Netty is an open-source, asynchronous event-driven network application framework for the rapid development of maintainable high-performance protocol servers & clients. In Netty (io.netty:netty-codec-http2) before version 4.1.61.Final, there is a vulnerability that enables request smuggling. The content-length header is not correctly validated if the request only uses a single Http2HeaderFrame with the endStream set to true. This could lead to request smuggling if the request is proxied to a remote peer and translated to HTTP/1.1. This is a follow-up of GHSA-wm47-8v5p-wjpj/CVE-2021-21295, which did miss to fix this one case.	CVE-2021-21409
The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.	CVE-2021-23358

Known CVE Issues in RM 10.0.4

The following table lists the known CVE issues in RM 10.0.4:

Description	CVE
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. ***Note:*** *This vulnerability is not exploitable because no user input is used in the validation rules, and it will be addressed in the following release.*	CVE-2020-10693
A flaw was found in Hibernate ORM. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SELECT or GROUP BY parts of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. ***Note:*** *This vulnerability is not exploitable because the vulnerability is in JPA API, and JRS does not use the JPA API; it uses the old search criteria API.*	CVE-2019-14900
A flaw was found in hibernate-core in versions prior to and including 5.4.23.Final. A SQL injection in the implementation of the JPA Criteria API can permit unsanitized literals when a literal is used in the SQL comments of the query. This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity. ***Note:*** *This vulnerability is not exploitable because the vulnerability is in JPA API, and JRS does not use the JPA API, it uses the old search criteria API.*	CVE-2020-25638

Description	CVE
Spring Security can fail to save the SecurityContext if it is changed more than once in a single request.A malicious user cannot cause the bug to happen (it must be programmed in). However, if the application's intent is to only allow the user to run with elevated privileges in a small portion of the application, the bug can be leveraged to extend those privileges to the rest of the application. ***Note:*** *It does not affect the Server in any way because the SecurityContext is never set more than once for any request in the application.*	CVE-2021-22112
Spring Security is vulnerable to side-channel attacks. Vulnerable versions of Spring Security don't use constant time comparisons for CSRF tokens. ***Note:*** *The attack is merely "theoretical". The Spring Security team confirms that it is not practical, in the logged issue: https://github.com/spring-projects/spring-security/issues/9291.* The attack is based on an assumption that the attacker somehow can measure the time it takes to compare two strings (in this case, CSRF tokens, a received one and the reference), and guess the string based on the fact that the default comparison algorithm would take longer to execute as more leading characters match between the strings. CSRF tokens are relatively short, and the time to compare will be totally diluted by other operations in a request. The attacker cannot measure only comparison specific time without virtually full control of the server and the running JVM.	WS-2020-0293