Ataccama Security Advisories

June 2025

Version latest, 2025-08-20

Table of Contents

Ataccama Security Advisories

This article lists the fixed security vulnerabilities that could have an impact on Ataccama products as well as their remediation.

Updates are published at the beginning of each month. The version number indicates in which release the fix was delivered.

June 2025

Version 16.2.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2024-21147: openjdk/17.0.10+7
  - CVE-2024-38819 (GHSA-g5vr-rgqm-vf78): spring-webflux/6.1.13, spring-webmvc/6.1.13
  - CVE-2024-38821 (GHSA-c4q5-6c82-3qpw): spring-security-web/6.3.3
  - CVE-2024-43598 (GHSA-2586-f3p4-hq84): lightgbm/3.3.5
  - CVE-2024-49203 (GHSA-6q3q-6v5j-h6vg): querydsl-jpa/5.1.0
  - CVE-2024-50379 (GHSA-5j33-cvvr-w245): tomcat-embed-core/10.1.25,30,31
  - CVE-2024-56406: libperl5.36/5.36.0-7+deb12u1, perl-base/5.36.0-7+deb12u1, perl-modules-5.36/5.36.0-7+deb12u1, perl/5.36.0-7+deb12u1
- **ONE, MDM (AI Matching)**
  - CVE-2024-47874 (GHSA-f96h-pmfr-66vw): starlette/0.36.3, starlette/0.37.2
  - CVE-2024-8176: libexpat1/2.6.3-1, libexpat1/2.6.4-1
  - CVE-2025-0395: libc-bin/2.40-2,3, libc6/2.40-2,3, libc6-dev/2.40-2, libc-dev-bin/2.40-2
  - CVE-2025-29087: libsqlite3-0/3.46.0-1, libsqlite3-0/3.46.1-1
  - CVE-2025-31115: liblzma5/5.6.2-2, liblzma5/5.6.3-1+b1
  - CVE-2025-43859 (GHSA-vqfr-h8mv-ghfj): h11/0.14.0
- **MDM**
  - CVE-2025-24789 (GHSA-7hpq-3g6w-pvhf): snowflake-jdbc/3.13.29
- **MDM, RDM**
  - CVE-2024-7254 (GHSA-735f-pc8j-v9w8): protobuf-java/3.21.12
- **ONE, MDM, RDM**
  - CVE-2024-56337 (GHSA-27hp-xhwr-wr2m): tomcat-embed-core/10.1.25,30,31
  - CVE-2025-24813 (GHSA-83qj-6fr2-vhqg): tomcat-embed-core/10.1.25,30,31
  - CVE-2025-24970 (GHSA-4g8c-wm8x-jfhw): netty-handler/4.1.109-110,112-114.Final

- CVE-2025-22235 (GHSA-rc42-6c7j-7h5r): spring-boot/3.2.5, 3.2.10-11, 3.3.4-5

- **ONE, MDM, RDM, DQIT**
  - CVE-2024-57699 (GHSA-pq2g-wx69-c263): json-smart/2.5.1
  - CVE-2025-21587: openjdk/17.0.10+7, openjdk/17.0.12+7, openjdk/17.0.14+7, openjdk/21.0.4+7-LTS
  - CVE-2025-22228 (GHSA-mg83-c7gq-rv5c): spring-security-crypto/6.3.3,4

May 2025

Version 15.4.1

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2024-4741: libcrypto3/3.1.4-r5, libssl3/3.1.4-r5
  - CVE-2024-5535: libcrypto3/3.1.4-r5, libssl3/3.1.4-r5
  - CVE-2024-6119: libcrypto3/3.1.4-r5, libssl3/3.1.4-r5
  - CVE-2024-21147: openjdk/17.0.10+7
  - CVE-2024-38819 (GHSA-g5vr-rgqm-vf78): spring-webflux/6.1.13, spring-webmvc/6.1.13
  - CVE-2024-38821 (GHSA-c4q5-6c82-3qpw): spring-security-web/6.3.3
  - CVE-2024-43598 (GHSA-2586-f3p4-hq84): lightgbm/3.3.5
  - CVE-2024-49203 (GHSA-6q3q-6v5j-h6vg): querydsl-jpa/5.1.0
  - CVE-2024-56406: libperl5.36/5.36.0-7+deb12u1, perl-base/5.36.0-7+deb12u1, perl-modules-5.36/5.36.0-7+deb12u1, perl/5.36.0-7+deb12u1
  - CVE-2025-26519: musl-utils/1.2.4_git20230717-r4, musl/1.2.4_git20230717-r4
- **ONE, MDM, RDM**
  - CVE-2024-50379 (GHSA-5j33-cvvr-w245): tomcat-embed-core/10.1.25,30,31
  - CVE-2024-56337 (GHSA-27hp-xhwr-wr2m): tomcat-embed-core/10.1.25,30,31
  - CVE-2025-22235 (GHSA-rc42-6c7j-7h5r): spring-boot/3.2.10,11, /3.2.5, /3.3.1,4,5
  - CVE-2025-24813 (GHSA-83qj-6fr2-vhqg): tomcat-embed-core/10.1.25,30,31
  - CVE-2025-24970 (GHSA-4g8c-wm8x-jfhw): netty-handler/4.1.109-110.Final, netty-handler/4.1.112-114.Final
- **ONE, MDM, RDM, DQIT**
  - CVE-2024-57699 (GHSA-pq2g-wx69-c263): json-smart/2.5.1
  - CVE-2025-21587: openjdk/17.0.10+7, openjdk/17.0.12+7, openjdk/17.0.14+7, openjdk/21.0.4+7-LTS
  - CVE-2025-22228 (GHSA-mg83-c7gq-rv5c): spring-security-crypto/6.3.3,4

- **ONE, MDM (AI Matching)**
  - CVE-2024-8176: libexpat1/2.6.3-1, libexpat1/2.6.4-1
  - CVE-2024-47874 (GHSA-f96h-pmfr-66vw): /0.37.2, starlette/0.36.3
  - CVE-2025-0395: libc-bin/2.40-2,3 libc-dev-bin/2.40-2, libc6-dev/2.40-2, libc6/2.40-2,3
  - CVE-2025-29087: libsqlite3-0/3.46.0-1, libsqlite3-0/3.46.1-1
  - CVE-2025-31115: liblzma5/5.6.2-2, liblzma5/5.6.3-1+b1
  - CVE-2025-43859 (GHSA-vqfr-h8mv-ghfj): h11/0.14.0
- **MDM**
  - CVE-2025-24789 (GHSA-7hpq-3g6w-pvhf): snowflake-jdbc/3.13.29
- **MDM, RDM**
  - CVE-2024-7254 (GHSA-735f-pc8j-v9w8): protobuf-java/3.21.12

April 2025

Version 16.1.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2024-38819 (GHSA-g5vr-rgqm-vf78): spring-webflux/6.1.13, spring-webmvc/6.1.13
  - CVE-2024-43598 (GHSA-2586-f3p4-hq84): lightgbm/3.3.5
  - CVE-2024-47554 (GHSA-78wr-2p64-hpwj): commons-io/2.11.0
  - CVE-2024-49203 (GHSA-6q3q-6v5j-h6vg): querydsl-jpa/6.9
  - CVE-2024-50379 (GHSA-5j33-cvvr-w245): tomcat-catalina/10.1.33, tomcat-embed-core/10.1.25,31,33
  - CVE-2024-56337 (GHSA-27hp-xhwr-wr2m): tomcat-catalina/10.1.33, tomcat-embed-core/10.1.25,31,33
  - CVE-2025-1094: libpq-dev/15.10-0+deb12u1, libpq5/15.10-0+deb12u1, postgresql-client-15/15.10-0+deb12u1
  - CVE-2025-26519: musl-utils/1.2.5-r0, musl/1.2.5-r0
- **ONE, MDM, RDM**
  - CVE-2025-22228 (GHSA-mg83-c7gq-rv5c): spring-security-crypto/6.3.5,6
  - CVE-2025-24813 (GHSA-83qj-6fr2-vhqg): tomcat-catalina/10.1.33,34 tomcat-embed-core/10.1.25,31,33,34
  - CVE-2025-24970 (GHSA-4g8c-wm8x-jfhw): netty-handler/4.1.114.Final, netty-handler/4.1.115.Final, netty-handler/4.1.116.Final
- **ONE, MDM, RDM, DQIT**

    - CVE-2024-57699 (GHSA-pq2g-wx69-c263): json-smart/2.5.1
- **ONE, MDM (AI Matching)**
    - CVE-2025-0395: libc-bin/2.40-3, libc-dev-bin/2.40-3, libc6-dev/2.40-3, libc6/2.40-3
- **MDM**
    - CVE-2025-24789 (GHSA-7hpq-3g6w-pvhf): snowflake-jdbc/3.13.29

March 2025

CVE-2025-24813 in Apache Tomcat

Ataccama products are not affected by the CVE-2025-24813 vulnerability in Apache Tomcat if default product configurations are used.

The vulnerability, which can lead to remote code execution or information disclosure, can only be exploited if all of the following conditions are met:

1. **Writes are enabled for the default servlet**: This feature is turned off by default.
2. **Support for partial PUT**: This feature is turned on by default.
3. **The given application uses Tomcat file-based session persistence with the default storage location**.
4. **The given application includes a library that can be leveraged in a deserialization attack**.

After a thorough review, we can confirm that our products do not meet these conditions.

The CVE will be fixed in the upcoming releases, namely 15.4.1 and 16.1.0. In addition, we are preparing release patches for versions 14.5.3, 15.4.0, and 16.0.0.

If you are using a version earlier than 14.5.x LTS, we encourage you to upgrade so you can benefit from the latest patches.

If you have further questions or you require assistance, contact Ataccama Support team.

January 2025

Version 16.0.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
    - CVE-2024-21147: openjdk/17.0.10+7
    - CVE-2024-38819 (GHSA-g5vr-rgqm-vf78): spring-webmvc/6.1.13, spring-webflux/6.1.13
    - CVE-2024-38821 (GHSA-c4q5-6c82-3qpw): spring-security-web/6.3.3
- **ONE, MDM (AI Matching)**

- CVE-2024-47874 (GHSA-f96h-pmfr-66vw): starlette/0.36.3, starlette/0.37.2

- **MDM, RDM**
  - CVE-2024-7254 (GHSA-735f-pc8j-v9w8): protobuf-java/3.21.12
  - CVE-2024-50379 (GHSA-5j33-cvvr-w245): tomcat-embed-core/10.1.31
  - CVE-2024-56337 (GHSA-27hp-xhwr-wr2m): tomcat-embed-core/10.1.31
- **DQIT**
  - CVE-2023-6841 (GHSA-w97f-w3hq-36g2): keycloak-core/23.0.7
  - (GHSA-93ww-43rr-79v3): keycloak-core/23.0.7

November 2024

Version 15.4.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2020-16156: perl-base/5.32.1-4+deb11u3
  - CVE-2021-33560: libgcrypt20/1.8.7-6
  - CVE-2021-36690: libsqlite3-0/3.34.1-3
  - CVE-2022-1304: e2fsprogs/1.46.2-2, libcom-err2/1.46.2-2, libext2fs2/1.46.2-2, libss2/1.46.2-2, logsave/1.46.2-2
  - CVE-2022-3715: bash/5.1-2+deb11u1
  - CVE-2022-4899: libzstd1/1.4.8+dfsg-2.1
  - CVE-2022-42916: curl/7.74.0-1.3+deb11u12, libcurl4/7.74.0-1.3+deb11u12
  - CVE-2022-43551: curl/7.74.0-1.3+deb11u12, libcurl4/7.74.0-1.3+deb11u12
  - CVE-2023-44487: libnghttp2-14/1.43.0-1build3
  - CVE-2024-0553: libgnutls30/3.7.9-2+deb12u3
  - CVE-2024-0567: libgnutls30/3.7.9-2+deb12u3
  - CVE-2024-6345 (GHSA-cx63-2mw6-8hw5): setuptools/65.5.0-1
  - CVE-2024-20918: openjdk/17.0.8.1+1, openjdk/17.0.9+9
  - CVE-2024-20932: openjdk/17.0.8.1+1, openjdk/17.0.9+9
  - CVE-2024-20952: openjdk/17.0.8.1+1, openjdk/17.0.9+9
  - CVE-2024-22262 (GHSA-2wrp-6fg6-hmc5): spring-web/6.1.5
  - CVE-2024-40094 (GHSA-h9mq-f6q5-6c8m): graphql-java/20.8, 21.3, 21.4
  - CVE-2022-40897 (GHSA-r9hx-vwmv-q579): setuptools/65.5.0
  - CVE-2024-47874 (GHSA-f96h-pmfr-66vw): starlette/0.36.3

- CVE-2024-52804 (GHSA-8w49-h785-mj3c): tornado/6.4.1

- **ONE, MDM**
  - CVE-2024-7254 (GHSA-735f-pc8j-v9w8): protobuf-java/3.21.12, 3.24.0, 3.25.1, 3.25.3, 3.25.4, protobuf-kotlin/3.21.12
  - CVE-2023-23914: curl/7.74.0-1.3+deb11u12, libcurl4/7.74.0-1.3+deb11u12
  - CVE-2024-43805 (GHSA-9q39-rmj3-p4r2): jupyterlab/4.2.2, notebook/7.2.1
  - CVE-2024-47561 (GHSA-r7pg-v2c8-mfg3): avro/1.11.3
- **ONE, MDM, RDM**
  - CVE-2024-21147: openjdk/17.0.8.1+1, 17.0.9+9, 17.0.10+7, 17.0.11+9
  - CVE-2024-38816 (GHSA-cx7f-g6mp-7hqm): spring-webflux/6.0.13, 6.1.6, 6.1.11, spring-webmvc/6.1.5-6, 6.1.10-11
- **ONE, MDM, RDM, DQIT**
  - CVE-2024-38821 (GHSA-c4q5-6c82-3qpw): spring-security-web/6.2.4, 6.3.1
- **ONE, MDM, DQIT**
  - CVE-2024-47554 (GHSA-78wr-2p64-hpwj): commons-io/2.10.0, 2.11.0
- **ONE, MDM (AI Matching)**
  - CVE-2024-37370: libgssapi-krb5-2/1.20.1-2,1.20.1-2+deb12u1, libk5crypto3/1.20.1-2,1.20.1-2+deb12u1, libkrb5-3/1.20.1-2,1.20.1-2+deb12u1, libkrb5support0/1.20.1-2,1.20.1-2+deb12u1
  - CVE-2024-37371: ibgssapi-krb5-2/1.20.1-2,1.20.1-2+deb12u1, libk5crypto3/1.20.1-2,1.20.1-2+deb12u1, libkrb5-3/1.20.1-2,1.20.1-2+deb12u1, libkrb5support0/1.20.1-2,1.20.1-2+deb12u1
- **ONE, MDM (AI Matching), Data Stories**
  - CVE-2024-45490: libexpat/2.6.2-r0, libexpat1/2.2.10-2+deb11u5, 2.6.2-1
  - CVE-2024-45491: libexpat/2.6.2-r0, libexpat1/2.2.10-2+deb11u5, 2.6.2-1
  - CVE-2024-45492: libexpat/2.6.2-r0, libexpat1/2.2.10-2+deb11u5, 2.6.2-1
- **ONE, DQIT**
  - CVE-2024-34750 (GHSA-wm9w-rjj3-j356): tomcat-embed-core/10.1.19-20, tomcat-coyote/10.1.18
- **MDM**
  - CVE-2019-8457: libdb5.3/5.3.28+dfsg1-0.8
- **MDM (AI Matching)**
  - CVE-2024-5535: libssl3t64/3.2.2-1, openssl/3.2.2-1
- **MDM (AI Matching), Data Stories**
  - CVE-2024-6119: libcrypto3/3.3.1-r3, libssl3/3.3.1-r3, libssl3t64/3.2.2-1, openssl/3.2.2-1
- **DQIT**
  - CVE-2024-34156: stdlib/go1.22.5
  - CVE-2024-34158: stdlib/go1.22.5

- CVE-2024-38286 (GHSA-7jqf-v358-p8g7): tomcat-util/10.1.18

August 2024

Version 15.3.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2020-22218: libssh2-1/1.9.0-2
  - CVE-2023-0464: libssl1.1/1.1.1n-0+deb11u4, openssl/1.1.1n-0+deb11u4
  - CVE-2023-4911: libc-bin/2.31-13+deb11u6, 2.36-9+deb12u1, libc6/2.31-13+deb11u6, 2.36-9+deb12u1
  - CVE-2023-5363: libssl3/3.0.9-1, openssl/3.0.9-1
  - CVE-2023-6246: libc-bin/2.36-9+deb12u1, 2.36-9+deb12u3, libc6/2.36-9+deb12u1, 2.36-9+deb12u3
  - CVE-2023-6779: libc-bin/2.36-9+deb12u1, 2.36-9+deb12u3, libc6/2.36-9+deb12u1, 2.36-9+deb12u3
  - CVE-2023-24329: python/3.11.3
  - CVE-2023-29491: libncursesw6/6.2+20201114-2+deb11u1, libtinfo6/6.2+20201114-2+deb11u1, ncurses-bin/6.2+20201114-2+deb11u1
  - CVE-2023-36632: python/3.11.3
  - CVE-2023-41105: python/3.11.3
  - CVE-2023-47038: perl-base/5.32.1-4+deb11u2, perl-base/5.36.0-7
  - CVE-2024-0553: libgnutls30/3.7.1-5+deb11u3
  - CVE-2024-0567: libgnutls30/3.7.1-5+deb11u3
  - CVE-2024-7348: libpq-dev/13.14-0+deb11u1, libpq5/13.14-0+deb11u1, postgresql-client-13/13.14-0+deb11u1
  - CVE-2024-22243 (GHSA-ccgv-vj62-xf9h): spring-web/6.1.3
  - CVE-2024-23342 (GHSA-wj6h-64fc-37mp): ecdsa/0.18.0
  - CVE-2024-25638 (GHSA-cfxw-4h78-h7fw): dnsjava/2.1.7
  - CVE-2024-33663 (GHSA-6c5p-j8vq-pqhj): python-jose/3.3.0
  - CVE-2024-35178 (GHSA-hrw6-wg82-cm62): jupyter-server/2.7.0
  - CVE-2024-39705 (GHSA-cgvx-9447-vcch): nltk/3.8.1
- **ONE, MDM**
  - CVE-2023-44487: libnghttp2-14/1.43.0-1build3
- **ONE, MDM, RDM**

- CVE-2024-25710 (GHSA-4g9r-vxhx-9pgx): commons-compress/1.25.0
- CVE-2024-34750 (GHSA-wm9w-rjj3-j356): tomcat-embed-core/10.1.16,18,19,20
- CVE-2024-40094 (GHSA-h9mq-f6q5-6c8m): graphql-java/18.7, 21.3-4

- **ONE, MDM, RDM, DQIT**
  - CVE-2024-22262 (GHSA-2wrp-6fg6-hmc5): spring-web/6.1.3,4,5
- **ONE, MDM, DQIT**
  - CVE-2024-20918: java/jre/17.0.8.1+1, 17.0.9+9, 21.0.1+12-LTS
  - CVE-2024-20952: java/jre/17.0.8.1+1, 17.0.9+9, 21.0.1+12-LTS
- **ONE, MDM (AI Matching)**
  - CVE-2023-31484: perl-base/5.36.0-7, 5.36.0-7+deb12u1
- **ONE, MDM (AI Matching), Data Stories**
  - CVE-2023-7104: libsqlite3-0/3.40.1-2
  - CVE-2023-45853: zlib1g/1:1.2.13.dfsg-1, 1:1.3.dfsg-3+b1
  - CVE-2023-50387: libsystemd0/252.12-1~deb12u1, 252.17-1~deb12u1, 252.19-1~deb12u1, 252.22-1~deb12u1, libudev1/252.12-1~deb12u1, 252.17-1~deb12u1, 252.19-1~deb12u1, 252.22-1~deb12u1
  - CVE-2023-52425: libexpat/2.5.0-1, 2.5.0-r2
  - CVE-2024-6345 (GHSA-cx63-2mw6-8hw5): setuptools/65.5.1, 67.4.0, 67.7.2, 68.2.2, 69.1.1
  - CVE-2024-2961: libc-bin/2.31-13+deb11u6, 2.36-9+deb12u1,3,4, libc6/2.31-13+deb11u6, 2.36-9+deb12u1,3,4
  - CVE-2024-33601: libc-bin/2.31-13+deb11u6, 2.36-9+deb12u1,3,4, libc6/2.31-13+deb11u6, 2.36-9+deb12u1,3,4
  - CVE-2024-33602: libc-bin/2.31-13+deb11u6, 2.36-9+deb12u1,3,4, libc6/2.31-13+deb11u6, 2.36-9+deb12u1,3,4
- **ONE, Data Stories**
  - CVE-2023-6597: python/3.11.3,7
  - CVE-2024-2398: curl/7.74.0-1.3+deb11u11, 8.5.0-r0, libcurl/8.5.0-r0, libcurl4/7.74.0-1.3+deb11u11
  - CVE-2024-30251 (GHSA-5m98-qgg9-wh84): aiohttp/3.9.1,3
  - CVE-2024-37370: libgssapi-krb5-2/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libk5crypto3/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libkrb5-3/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libkrb5support0/1.18.3-6+deb11u3, 1.20.1-2+deb12u1
  - CVE-2024-37371: libgssapi-krb5-2/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libk5crypto3/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libkrb5-3/1.18.3-6+deb11u3, 1.20.1-2+deb12u1, libkrb5support0/1.18.3-6+deb11u3, 1.20.1-2+deb12u1
- **ONE, DQIT**
  - CVE-2024-20932: java/jre/17.0.8.1+1, 17.0.9+9

- **MDM**
  - CVE-2024-1597 (GHSA-24rp-q3w6-vc56): postgresql/42.6.0
  - CVE-2024-21147: java/jre/21.0.1+12-LTS
  - CVE-2024-22234 (GHSA-w3w6-26f2-p474): spring-security-core/6.2.1
  - CVE-2024-38816 (GHSA-cx7f-g6mp-7hqm): spring-webmvc/6.1.3
- **MDM, DQIT**
  - CVE-2024-22257 (GHSA-f3jh-qvm4-mg39): spring-security-core/6.2.1,2
  - CVE-2024-22259 (GHSA-hgjh-9rj2-g67j): spring-web/6.1.3,4
- **Data Stories**
  - CVE-2023-2953: libldap-2.5-0/2.5.13+dfsg-5+b3
  - CVE-2024-5535: libssl-dev/3.2.1-3, libssl3t64/3.2.1-3, openssl/3.2.1-3
  - CVE-2024-6197: curl/8.5.0-r0, libcurl/8.5.0-r0
  - CVE-2024-25062: libxml2/2.11.6-r0
  - CVE-2024-34459: libxml2/2.11.6-r0
  - CVE-2024-38428: wget/1.21.4-r0
  - CVE-2024-38875 (GHSA-qg2p-9jwr-mmqf): django/4.2.11
  - CVE-2024-39330 (GHSA-9jmf-237g-qf46): django/4.2.11
  - CVE-2024-39614 (GHSA-f6f8-9mx6-9mx2): django/4.2.11
  - CVE-2024-42005 (GHSA-pv4p-cwwg-4rph): django/4.2.11
  - CVE-2024-45490: libexpat1/2.5.0-1
  - CVE-2024-45491: libexpat1/2.5.0-1
  - CVE-2024-45492: libexpat1/2.5.0-1
- **DQIT**
  - CVE-2023-45288: stdlib/go1.21.6
  - CVE-2024-24784: stdlib/go1.21.6
  - CVE-2024-24790: stdlib/go1.21.6
  - CVE-2024-24791: stdlib/go1.21.6

June 2024

CVE-2024-1597 in PostgreSQL driver

CVE-2024-1597 has not been fixed in DQIT version 14.5.3. While DQIT uses PostgreSQL, it is not exposed to the vulnerability since the PostgreSQL driver is vulnerable only if using `PreferQueryMode=SIMPLE`, which is not implemented in DQIT.

Therefore, no customer action is required.

The issue will be fixed in DQIT version 14.5.4 and is already fixed in version 15.2.0.

Version 14.5.3

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2023-2953: libldap-2.5-0/2.5.13+dfsg-5
  - CVE-2023-4785 (GHSA-p25m-jpj4-qcrr): grpcio/1.54.0
  - CVE-2023-6481 (GHSA-gm62-rw4g-vrc4): logback-core/1.3.13, 1.4.13
  - CVE-2023-6597: python/3.11.6
  - CVE-2023-7104: libsqlite3-0/3.40.1-2
  - CVE-2023-50387: libsystemd0/252.17-1~deb12u1, libudev1/252.17-1~deb12u1
  - CVE-2023-52425: libexpat1/2.5.0-1
  - CVE-2024-25710 (GHSA-4g9r-vxhx-9pgx): commons-compress/1.21, 1.23.0, 1.24.0
  - CVE-2024-26308 (GHSA-4265-ccf5-phj5): commons-compress/1.21, 1.23.0, 1.24.0
- **ONE, MDM**
  - CVE-2024-21634 (GHSA-264p-99wq-f4j6): ion-java/1.0.2
- **ONE, MDM, RDM**
  - CVE-2023-34053 (GHSA-v94h-hvhg-mf9h): spring-webmvc/6.0.11-13
  - CVE-2023-46589 (GHSA-fccv-jmmp-qg76): tomcat-embed-core/10.1.12,13,15
  - CVE-2024-1597 (GHSA-24rp-q3w6-vc56): postgresql/42.5.4, 42.6.0, 42.7.0
  - CVE-2024-22234 (GHSA-w3w6-26f2-p474): spring-security-core/6.1.3-5
  - CVE-2024-22262 (GHSA-2wrp-6fg6-hmc5): spring-web/6.0.11,13,14
- **ONE, MDM, RDM, DQIT**
  - CVE-2024-20918: java/jre/17.0.8.1+1
  - CVE-2024-20932: java/jre/17.0.8.1+1
  - CVE-2024-20952: java/jre/17.0.8.1+1
  - CVE-2024-22243 (GHSA-ccgv-vj62-xf9h): spring-web/5.3.30, 6.0.11,13,14
  - CVE-2024-22257 (GHSA-f3jh-qvm4-mg39): spring-security-core/5.7.11, 6.1.3-5
  - CVE-2024-22259 (GHSA-hgjh-9rj2-g67j): spring-web/5.3.30, 6.0.11,13,14
- **ONE, MDM (AI Matching), Data Stories**
  - CVE-2023-6246: libc6/2.36-9+deb12u3, libc-bin/2.36-9+deb12u3
  - CVE-2023-6779: libc6/2.36-9+deb12u3, libc-bin/2.36-9+deb12u3
  - CVE-2023-50782 (GHSA-3ww4-gg4f-jr7f): cryptography/41.0.7
  - CVE-2024-0553: libgnutls30/3.7.9-2

- CVE-2024-0567: libgnutls30/3.7.9-2
- CVE-2024-24762 (GHSA-2jv5-9r88-3w3p): fastapi/0.95.2,0.101.0, starlette/0.27.0
- CVE-2024-26130 (GHSA-6vqw-3v5j-54x4): cryptography/41.0.7

- **ONE, Data Stories**
  - CVE-2023-6022 (GHSA-4hh5-2678-83fx): prefect/2.14.8
  - CVE-2024-4340 (GHSA-2m57-hf25-phgg): sqlparse/0.4.4
  - CVE-2024-23342 (GHSA-pwr2-4v36-6qpr): orjson/3.9.4
  - CVE-2024-23342 (GHSA-wj6h-64fc-37mp): ecdsa//0.17.0, 0.18.0
  - CVE-2024-30251 (GHSA-5m98-qgg9-wh84): aiohttp/3.9.1
  - CVE-2024-33663 (GHSA-6c5p-j8vq-pqhj): python-jose/3.3.0
- **MDM**
  - CVE-2023-5363: libcrypto3/3.1.3-r0, libssl3/3.1.3-r0
  - CVE-2023-34054 (GHSA-q24v-hpg3-v3jp): reactor-netty-http/1.1.12
  - CVE-2023-34062 (GHSA-xjhv-p3fv-x24r): reactor-netty-http/1.1.12
- **MDM, RDM**
  - CVE-2021-22569 (GHSA-wrvw-hg22-4m67): protobuf-java/2.5.0
  - CVE-2021-22570 (GHSA-77rm-9x9h-xj3g): protobuf-java/2.5.0
  - CVE-2022-3509 (GHSA-g5ww-5jh7-63cx): protobuf-java/2.5.0
  - CVE-2022-3510 (GHSA-4gg5-vx3j-xwc7): protobuf-java/2.5.0
  - CVE-2023-6378 (GHSA-vmq6-5m68-f53m): logback-classic/1.4.11, logback-core/1.4.11
- **MDM (AI Matching)**
  - CVE-2023-47038: perl-base/5.36.0-7
- **DQIT**
  - CVE-2023-24998 (GHSA-hfrx-6qgj-fp6c): tomcat-coyote/9.0.69

May 2024

Version 15.2.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2023-4785 (GHSA-p25m-jpj4-qcrr): grpcio/1.54.0
  - CVE-2023-6481 (GHSA-gm62-rw4g-vrc4): logback-core/1.4.13
  - CVE-2024-0985: libpq-dev/13.13-0+deb11u1, libpq5/13.13-0+deb11u1, postgresql-client-13/13.13-0+deb11u1

- CVE-2023-34053 (GHSA-v94h-hvhg-mf9h): spring-webmvc/6.0.13
- CVE-2023-46589 (GHSA-fccv-jmmp-qg76): tomcat-embed-core/10.1.15
- CVE-2023-50447 (GHSA-3f63-hfp8-52jq): Pillow/10.0.1
- CVE-2024-20918: java/jre/17.0.8.1+1
- CVE-2024-20952: java/jre/17.0.8.1+1
- CVE-2024-22233 (GHSA-r4q3-7g4q-x89m): spring-core/6.0.15
- CVE-2024-25710 (GHSA-4g9r-vxhx-9pgx): commons-compress/1.23.0, 1.24.0, 1.25.0
- CVE-2024-26308 (GHSA-4265-ccf5-phj5): commons-compress/1.23.0, 1.24.0, 1.25.0
- CVE-2024-29415 (GHSA-2p57-rm9w-gvfp): ip/2.0.0

- **ONE, MDM**
  - CVE-2023-5363: libcrypto3/3.1.2-r0, 3.1.3-r0, libssl3/3.1.2-r0, 3.1.3-r0
  - CVE-2024-21634 (GHSA-264p-99wq-f4j6): ion-java/1.0.2
  - CVE-2024-22262 (GHSA-2wrp-6fg6-hmc5): spring-web/6.0.13-14, 6.1.1
- **ONE, MDM (AI Matching)**
  - CVE-2024-0553: libgnutls30/3.7.9-2, 3.7.9-2+deb12u1
  - CVE-2024-0567: libgnutls30/3.7.9-2, 3.7.9-2+deb12u1
- **ONE, Data Stories**
  - CVE-2024-27454 (GHSA-pwr2-4v36-6qpr): orjson/3.9.1, 3.9.10
- **ONE, MDM (AI Matching), Data Stories**
  - CVE-2023-50782 (GHSA-3ww4-gg4f-jr7f): cryptography/41.0.7
  - CVE-2024-24762 (GHSA-2jv5-9r88-3w3p): fastapi/0.95.2, 0.104.0-1, 0.108.0, starlette/0.27.0, 0.32.0.post1
  - CVE-2024-26130 (GHSA-6vqw-3v5j-54x4): cryptography/41.0.7, 42.0.0
- **ONE, MDM, RDM**
  - CVE-2024-20932: java/jre/17.0.8.1+1, java/jre/17.0.9+9
  - CVE-2024-22234 (GHSA-w3w6-26f2-p474): spring-security-core/6.1.5, 6.2.0
  - CVE-2024-22257 (GHSA-f3jh-qvm4-mg39): spring-security-core/6.1.5, 6.2.0
  - CVE-2024-22259 (GHSA-hgjh-9rj2-g67j): spring-web/6.0.13-15, 6.1.1, 6.1.3
- **ONE, MDM, RDM, DQIT**
  - CVE-2024-1597 (GHSA-24rp-q3w6-vc56): postgresql/42.4.1, 42.6.0, 42.7.0, 42.7.1
  - CVE-2024-22243 (GHSA-ccgv-vj62-xf9h): spring-web/5.3.31, 6.0.13-15, 6.1.1, 6.1.3
- **MDM (AI Matching), Data Stories**
  - CVE-2023-6246: libc-bin/2.36-9+deb12u3, libc6/2.36-9+deb12u3
  - CVE-2023-6779: libc-bin/2.36-9+deb12u3, libc6/2.36-9+deb12u3
- **Data Stories**

    - CVE-2024-23342 (GHSA-wj6h-64fc-37mp): ecdsa/0.17.0
    - CVE-2024-33663 (GHSA-6c5p-j8vq-pqhj): python-jose/3.3.0
    - CVE-2024-4340 (GHSA-2m57-hf25-phgg): sqlparse/0.4.4
- **DQIT**
    - CVE-2016-1000027 (GHSA-4wrc-f8pq-fpqp): spring-web/5.3.31
    - CVE-2023-24998 (GHSA-hfrx-6qgj-fp6c): tomcat-coyote/9.0.69

February 2024

CVE-2023-30590, CVE-2023-32002, CVE-2023-39332 in OpenSearch Dashboards

Ataccama products use the OpenSearch Dashboards tool but are not exposed to the vulnerabilities CVE-2023-30590, CVE-2023-32002, and CVE-2023-39332 for the following reasons:

- CVE-2023-30590: OpenSearch Dashboards do not employ the critical `generateKeys()` API function returned from `crypto.createDiffieHellman()`.
- CVE-2023-32002: OpenSearch Dashboards do not employ the critical `--experimental-policy` flag when executing the Node.js binary.
- CVE-2023-39332: Affects versions of Node.js binaries prior to the one included in OpenSearch Dashboards distributed packages.

Therefore, no customer action is required.

For more information, see the following articles respectively:

- DiffieHellman do not generate keys after setting a private key (Medium) (CVE-2023-30590)
- Node.js Module-based permissions - Policies
- Installing OpenSearch Dashboards - Node.js compatibility

Version 14.5.2

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
    - CVE-2023-6246, CVE-2023-6779: libc-bin/2.36-9+deb12u3, libc6/2.36-9+deb12u3
    - CVE-2024-24762 (GHSA-2jv5-9r88-3w3p): fastapi/0.95.2, starlette/0.27.0
    - CVE-2023-50782 (GHSA-3ww4-gg4f-jr7f), CVE-2024-26130 (GHSA-6vqw-3v5j-54x4): cryptography/41.0.7
    - CVE-2023-4785 (GHSA-p25m-jpj4-qcrr): grpcio/1.54.0
- **ONE, DQIT**
    - CVE-2024-0553, CVE-2024-0567: gnutls/3.8.0-r2, libgnutls30/3.7.9-2

- **DQIT**
  - CVE-2022-48174: busybox-binsh/1.36.1-r0, busybox/1.36.1-r0, ssl_client/1.36.1-r0
  - CVE-2023-45285: stdlib/go1.20.11
  - CVE-2023-52425: libexpat/2.5.0-r1
  - CVE-2023-5363: libcrypto3/3.1.1-r1, libssl3/3.1.1-r1
  - CVE-2023-7104: sqlite-libs/3.41.2-r2
  - CVE-2024-24790: stdlib/go1.20.11, git/2.40.1-r0
  - CVE-2023-39325 (GHSA-4374-p667-p6c8): golang.org/x/net/v0.10.0

January 2024

Version 15.1.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2023-6481 (GHSA-gm62-rw4g-vrc4): logback-core/1.3.13, 1.4.13
- **ONE, MDM, RDM**
  - CVE-2023-34053 (GHSA-v94h-hvhg-mf9h): spring-webmvc/6.0.11-13
  - CVE-2023-46589 (GHSA-fccv-jmmp-qg76): tomcat-embed-core/10.1.12, 10.1.13, 10.1.15
- **ONE, MDM, RDM, DQIT**
  - CVE-2024-20918: java/jre/17.0.8.1+1
  - CVE-2024-20952: java/17.0.8.1+1, java/17.0.8.1+1-J-ms8m
- **ONE, Data Stories**
  - CVE-2023-6022 (GHSA-4hh5-2678-83fx): prefect/2.14.8
- **ONE, Data Stories, DQIT**
  - CVE-2024-0553: gnutls/3.8.0-r2, libgnutls30/3.7.9-2
  - CVE-2024-0567: gnutls/3.8.0-r2, libgnutls30/3.7.9-2
- **MDM**
  - CVE-2024-25710 (GHSA-4g9r-vxhx-9pgx): commons-compress/1.24.0
  - CVE-2024-26308 (GHSA-4265-ccf5-phj5): commons-compress/1.24.0
  - CVE-2023-34054 (GHSA-q24v-hpg3-v3jp): reactor-netty-http/1.1.12
  - CVE-2023-34062 (GHSA-xjhv-p3fv-x24r): reactor-netty-http/1.1.12
- **MDM (AI Matching)**
  - CVE-2023-47038: perl-base/5.36.0-7
- **MDM, RDM**

- CVE-2022-3509 (GHSA-g5ww-5jh7-63cx): protobuf-java/2.5.0
- CVE-2022-3510 (GHSA-4gg5-vx3j-xwc7): protobuf-java/2.5.0
- CVE-2021-22569 (GHSA-wrvw-hg22-4m67): protobuf-java/2.5.0
- CVE-2021-22570 (GHSA-77rm-9x9h-xj3g): protobuf-java/2.5.0

- **MDM, RDM, DQIT**
  - CVE-2023-6378 (GHSA-vmq6-5m68-f53m): logback-classic/1.4.11, logback-core/1.4.11
- **DQIT**
  - CVE-2023-5363: libcrypto3/3.1.1-r1, libssl3/3.1.1-r1
  - CVE-2023-7104: sqlite-libs/3.41.2-r2
  - CVE-2023-39323: stdlib/go1.21.1
  - CVE-2023-39325: stdlib/go1.21.1
  - CVE-2023-39325 (GHSA-4374-p667-p6c8): golang.org/x/net/v0.10.0
  - CVE-2023-44487: stdlib/go1.21.1
  - CVE-2023-45285: stdlib/go1.20.11, stdlib/go1.21.1
  - CVE-2022-48174: busybox/1.36.1-r0, busybox-binsh/1.36.1-r0, ssl_client/1.36.1-r0
  - CVE-2023-52425: libexpat/2.5.0-r1
  - CVE-2024-24790: stdlib/go1.20.11
  - CVE-2024-32002: git/2.40.1-r0
  - CVE-2024-32004: git/2.40.1-r0
  - CVE-2024-32465: git/2.40.1-r0

December 2023

CVE-2016-1000027 in Spring Framework

CVE-2016-1000027 has not been fixed in DQIT version 14.5.1. The vulnerability is related to Java remote code execution, which is not implemented in DQIT.

Therefore, no customer action is required.

The issue is fixed in DQIT version 15.2.0.

Version 14.5.1

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2019-17571 (GHSA-2qrg-x229-3v8q), CVE-2021-4104 (GHSA-fp5r-v3w9-4333), CVE-2022-23302 (GHSA-w9p3-5cr8-m3jj), CVE-2022-23305 (GHSA-65fg-84f6-3jq3), CVE-2022-23307

(GHSA-f7vh-qwp3-x37m): log4j/1.2.17

- CVE-2019-20444 (GHSA-cqqj-4p63-rrmm), CVE-2021-37136 (GHSA-grg4-wf29-r9vv), CVE-2021-37137 (GHSA-9vjp-v76f-g363): netty/3.10.6.Final
- CVE-2022-1471 (GHSA-mjmj-j48q-9wg2): snakeyaml/1.30, 33
- CVE-2022-25857 (GHSA-3mc7-4q67-w48m): snakeyaml/1.30
- CVE-2022-40150 (GHSA-x27m-9w8j-5vcw), CVE-2022-45685 (GHSA-7rf3-mqpx-h7xg), CVE-2022-45693 (GHSA-grr4-wv38-f68w), CVE-2023-1436 (GHSA-q6g2-g7f3-rr83): jettison/1.1
- CVE-2022-45688 (GHSA-3vqj-43w4-2q58): json/20210307
- CVE-2022-45868 (GHSA-22wj-vf5f-wrvj): h2/2.1.214
- CVE-2023-6246, CVE-2023-6779: libc-bin/2.36-9+deb12u1, libc6/2.36-9+deb12u1
- CVE-2023-6378 (GHSA-vmq6-5m68-f53m): logback-classic/1.2.12, 1.4.8, logback-core/1.2.12, 1.4.8
- CVE-2023-6597: python/3.11.5
- CVE-2023-0286: libssl3/3.0.2-0ubuntu1.7
- CVE-2023-1370 (GHSA-493p-pfq6-5258): json-smart/2.4.7
- CVE-2023-20883 (GHSA-xf96-w227-r7c4): spring-boot-autoconfigure/2.7.11
- CVE-2023-21930: java/jre/17.0.4.1+1
- CVE-2023-28867 (GHSA-p4qx-6w5p-4rj2): graphql-java/20.0
- CVE-2023-31582 (GHSA-7g24-qg88-p43q): jose4j/0.9.2
- CVE-2023-34034 (GHSA-3h6f-g5f3-gc4w): spring-security-config/5.7.8
- CVE-2023-34054 (GHSA-q24v-hpg3-v3jp), CVE-2023-34062 (GHSA-xjhv-p3fv-x24r): reactor-netty-http/1.0.32-33, 1.1.9
- CVE-2023-34981 (GHSA-mppv-79ch-vw6q): tomcat-embed-core/9.0.74
- CVE-2023-46589 (GHSA-fccv-jmmp-qg76): tomcat-embed-core/9.0.75
- CVE-2023-50387: libsystemd0/252.12-1~deb12u1, libudev1/252.12-1~deb12u1
- CVE-2023-50782 (GHSA-3ww4-gg4f-jr7f): cryptography/41.0.3
- CVE-2024-20918, CVE-2024-20952: java/jre/17.0.7+7
- CVE-2024-22257 (GHSA-f3jh-qvm4-mg39): spring-security-core/5.7.8
- CVE-2024-24762 (GHSA-2jv5-9r88-3w3p): fastapi/0.95.2, starlette/0.27.0
- CVE-2024-26130 (GHSA-6vqw-3v5j-54x4): cryptography/41.0.3

- **ONE, MDM**
  - CVE-2017-7525 (GHSA-qxxx-2pp7-5hmx), CVE-2017-15095 (GHSA-h592-38cm-4ggp), CVE-2017-17485 (GHSA-rfx6-vp9g-rh7v), CVE-2018-5968 (GHSA-w3f4-3q6j-rh82), CVE-2018-7489 (GHSA-cggj-fvv3-cqwv), CVE-2018-11307 (GHSA-qr7j-h6gg-jmgc), CVE-2018-12022 (GHSA-cjjf-94ff-43w7), CVE-2018-14718 (GHSA-645p-88qh-w398), CVE-2018-14719 (GHSA-4gq5-ch57-c2mg), CVE-2018-19362 (GHSA-c8hm-7hpq-7jhg), CVE-2019-12086 (GHSA-5ww9-j83m-q7qx), CVE-2019-14379 (GHSA-6fpp-rgj9-8rwc), CVE-2019-14439 (GHSA-gwp4-hfv6-p7hw), CVE-2019-

14540 (GHSA-h822-r4r5-v8jg), CVE-2019-14892 (GHSA-cf6r-3wgc-h863), CVE-2019-16335 (GHSA-85cw-hj65-qqv9), CVE-2019-16942 (GHSA-mx7p-6679-8g3q), CVE-2019-16943 (GHSA-fmmc-742q-jg75), CVE-2019-17267 (GHSA-f3j5-rmmp-3fc5), CVE-2019-17531 (GHSA-gjmw-vf9h-g25v), CVE-2019-20330 (GHSA-gww7-p5w4-wrfv), CVE-2020-8840 (GHSA-4w82-r329-3q67), CVE-2020-9547 (GHSA-q93h-jc49-78gg), CVE-2020-9548 (GHSA-p43x-xfjf-5jhr), CVE-2020-10650 (GHSA-rpr3-cw39-3pxh), CVE-2020-10673 (GHSA-fqwf-pjwf-7vqv), CVE-2020-24616 (GHSA-h3cw-g4mq-c5x2), CVE-2020-24750 (GHSA-qjw2-hr98-qgfh), CVE-2020-25649 (GHSA-288c-cq4h-88gq), CVE-2020-35490 (GHSA-wh8g-3j2c-rqj5), CVE-2020-35491 (GHSA-r3gr-cxrf-hg25), CVE-2020-35728 (GHSA-5r5r-6hpj-8gg9), CVE-2020-36179 (GHSA-9gph-22xh-8x98), CVE-2020-36180 (GHSA-8c4j-34r4-xr8g), CVE-2020-36181 (GHSA-cvm9-fjm9-3572), CVE-2020-36182 (GHSA-89qr-369f-5m5x), CVE-2020-36183 (GHSA-9m6f-7xcq-8vf8), CVE-2020-36184 (GHSA-m6x4-97wx-4q27), CVE-2020-36185 (GHSA-8w26-6f25-cm9x), CVE-2020-36186 (GHSA-v585-23hc-c647), CVE-2020-36187 (GHSA-r695-7vr9-jgc2), CVE-2020-36188 (GHSA-f9xh-2qgp-cq57), CVE-2020-36189 (GHSA-vfqx-33qm-g869), CVE-2020-36518 (GHSA-57j2-w4cx-62h2), CVE-2021-20190 (GHSA-5949-rw7g-wx7w), CVE-2022-42003 (GHSA-jjjh-jjxp-wpff), CVE-2022-42004 (GHSA-rgv9-q543-rqg4): jackson-databind/2.6.3

    - CVE-2021-22569 (GHSA-wrvw-hg22-4m67), CVE-2021-22570 (GHSA-77rm-9x9h-xj3g), CVE-2022-3509 (GHSA-g5ww-5jh7-63cx), CVE-2022-3510 (GHSA-4gg5-vx3j-xwc7): protobuf-java/2.5.0, 3.7.1
    - CVE-2022-36364 (GHSA-w7f5-jrpr-5c2m): avatica-core/1.11.0
    - CVE-2022-39135 (GHSA-fj2m-w3wv-x9pr): calcite-core/1.10.0
    - CVE-2023-4759 (GHSA-3p86-9955-h393): org.eclipse.jgit/5.13.1.202206130422-r
    - CVE-2023-34455 (GHSA-qcwq-55hx-v3vh): snappy-java/1.1.8.1, 1.1.8.4, 1.1.10.0
    - CVE-2023-39410 (GHSA-rhrv-645h-fjfh): avro/1.7.4, 1.7.7, 1.8.2, 1.10.1, 1.11.0
    - CVE-2023-40826 (GHSA-3r28-rgp9-qgv4), CVE-2023-40827 (GHSA-rvm8-j2cp-j592), CVE-2023-40828 (GHSA-cj8w-v588-p8wx): pf4j/3.0.1, 3.8.0
    - CVE-2023-43642 (GHSA-55g7-9cwv-5qfv): snappy-java/1.1.8.1,4, 1.1.10.0,1,3
    - CVE-2023-44981 (GHSA-7286-pgfv-vxvh): zookeeper/3.6.3
    - CVE-2023-46604 (GHSA-crg9-44h2-xw35): activemq-client/5.16.6
    - CVE-2024-36114 (GHSA-973x-65j7-xcf4): aircompressor/0.8
- **ONE, MDM, MDM (AI Matching), Data Stories, RDM**
    - CVE-2023-5363: libcrypto3/3.1.1-r1, libssl-dev/3.0.9-1, libssl3/3.0.9-1, libssl3/3.1.1-r1, openssl/3.0.9-1
- **ONE, MDM, MDM (AI Matching), Data Stories, RDM, DQIT**
    - CVE-2023-4911: libc-bin/2.35-0ubuntu3.1, 2.36-9+deb12u1, libc6-dev/2.36-9+deb12u1, libc6/2.35-0ubuntu3.1, 2.36-9+deb12u1, locales/2.35-0ubuntu3.1
- **ONE, MDM, Data Stories, RDM, DQIT**
    - CVE-2023-38039: curl/7.88.1-10+deb12u1, 8.2.1-r0, libcurl/8.2.1-r0, libcurl4/7.88.1-10+deb12u1
    - CVE-2023-38545: curl/7.81.0-1ubuntu1.6,10,13, 7.88.1-10+deb12u1, 8.2.1-r0, libcurl/8.2.1-r0, libcurl4/7.81.0-1ubuntu1.6,10,13, 7.88.1-10+deb12u1

- CVE-2023-44487: libnghttp2-14/1.52.0-1, nghttp2-libs/1.55.1-r0, stdlib/go1.20.7

- **ONE, MDM, RDM**
  - CVE-2016-1000027 (GHSA-4wrc-f8pq-fpqp): spring-web/5.3.27-29
  - CVE-2023-5072 (GHSA-4jq9-2xhw-jpx7): json/20210307, 20230618
  - CVE-2023-7104: libsqlite3-0/3.40.1-2, sqlite-libs/3.41.2-r2
  - CVE-2023-52425: libexpat1/2.5.0-1, libexpat/2.5.0-r1
  - CVE-2024-0553, CVE-2024-0567: libgnutls30/3.7.9-2, gnutls/3.8.0-r2
  - (GHSA-xpw8-rcwv-8f8p): netty-codec-http2/4.1.72.Final, 4.1.89.Final, 4.1.92.Final, 4.1.94.Final, 4.1.96.Final, 4.1.97.Final
- **ONE, MDM, RDM, DQIT**
  - CVE-2023-25193: java/jre/17.0.4.1+1, 17.0.6+10, 17.0.7+7
- **ONE, MDM (AI Matching)**
  - CVE-2023-4785 (GHSA-p25m-jpj4-qcrr): grpcio/1.54.0
- **ONE, MDM (AI Matching), Data Stories**
  - CVE-2023-36632, CVE-2023-41105: python/3.11.4
- **ONE, Data Stories**
  - CVE-2022-40897 (GHSA-r9hx-vwmv-q579): setuptools/65.5.0
  - CVE-2023-5869, CVE-2023-39417, CVE-2024-0985: libpq-dev/15.3-0+deb12u1, libpq5/15.3-0+deb12u1, postgresql-client-15/15.3-0+deb12u1
  - CVE-2023-31484, CVE-2023-47038: libperl5.36/5.36.0-7, perl-base/5.36.0-7, perl-modules-5.36/5.36.0-7, perl/5.36.0-7
  - CVE-2023-45853: zlib1g/1:1.2.13.dfsg-1
  - CVE-2023-46695 (GHSA-qmf9-6jqf-j8fq): Django/4.2.4
  - CVE-2023-49081 (GHSA-q3qx-c6g2-7pw2): aiohttp/3.8.5
- **Data Stories**
  - CVE-2023-47248 (GHSA-5wvp-7f3h-6wmm): pyarrow/10.0.1
- **MDM, RDM**
  - CVE-2022-48174: busybox-binsh/1.35.0-r27, 1.36.1-r0, busybox/1.35.0-r27, 1.36.1-r0, ssl_client/1.35.0-r27, 1.36.1-r0
  - CVE-2023-6481 (GHSA-gm62-rw4g-vrc4): logback-core/1.2.12
  - CVE-2023-39325 (GHSA-4374-p667-p6c8): golang.org/x/net/v0.10.0
  - CVE-2023-45285, CVE-2024-24790: stdlib/go1.20.7
  - CVE-2024-32002, CVE-2024-32004, CVE-2024-32465: git/2.40.1-r0
- **MDM, RDM, DQIT**
  - CVE-2023-39323: stdlib/go1.20.7

September 2023

Version 14.5.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking, sorted by modules:

- **ONE**
  - CVE-2007-2582: db2jcc4/4.31.10
  - CVE-2007-3676: db2jcc4/4.31.10
  - CVE-2007-5090: db2jcc4/4.31.10
  - CVE-2007-5652: db2jcc4/4.31.10
  - CVE-2008-3958: db2jcc4/4.31.10
  - CVE-2008-4692: db2jcc4/4.31.10
  - CVE-2011-0731: db2jcc4/4.31.10
  - CVE-2012-3324: db2jcc4/4.31.10
  - CVE-2023-0286: libssl3/3.0.2-0ubuntu1.7
  - CVE-2023-20860: spring-core/5.3.25
  - CVE-2023-3635: okio/2.8.0
  - CVE-2023-36632: python/3.9.16
  - CVE-2023-1370 (GHSA-493p-pfq6-5258): json-smart/2.4.7
  - CVE-2023-1428 (GHSA-6628-q6j9-w8vg): grpcio/1.51.3
- **ONE, MDM**
  - CVE-2023-32731 (GHSA-cfgp-2977-2fmm): grpcio/1.51.3
  - CVE-2023-2976: guava/31.1-jre
  - CVE-2023-34453: snappy-java/1.1.8.4
  - CVE-2023-34454: snappy-java/1.1.8.4
  - CVE-2023-34455: snappy-java/1.1.8.4
- **ONE, MDM (AI Matching)**
  - CVE-2022-40897 (GHSA-r9hx-vwmv-q579): setuptools/58.1.0
  - CVE-2022-29458: libncursesw6/6.2+20201114-2
- **ONE,Data Stories, MDM (AI Matching)**
  - CVE-2019-8457: libdb5.3/5.3.28+dfsg1-0.8
  - CVE-2020-16156: perl-base/5.32.1-4+deb11u2
  - CVE-2021-31239: libsqlite3-0/3.34.1-3
  - CVE-2021-33560: libgcrypt20/1.8.7-6

- CVE-2022-1304: e2fsprogs/1.46.2-2
- CVE-2022-3715: bash/5.1-2+deb11u1
- CVE-2022-4899: libzstd1/1.4.8+dfsg-2.1
- CVE-2023-0464: libssl1.1/1.1.1n-0+deb11u4
- CVE-2023-24329: python/3.11.3
- CVE-2023-29491: libncursesw6/6.2+20201114-2, libtinfo6/6.2+20201114-2+deb11u1
- CVE-2023-37920 (GHSA-xqr8-7jwr-rhp7): certifi/2023.5.7

- **ONE, Data Stories**
  - CVE-2023-38325 (GHSA-cf7p-gm2m-833m): cryptography/41.0.1
- **ONE, MDM, RDM, DQIT**
  - CVE-2023-30535 (GHSA-4g3j-c4wg-6j7x): snowflake-jdbc/3.13.26, snowflake-jdbc/3.13.14
  - CVE-2023-34034 (GHSA-3h6f-g5f3-gc4w): spring-security-core/5.7.8, spring-security-config/5.7.8
  - CVE-2020-7692 (GHSA-f263-c949-w85g): google-oauth-client/1.27.0
  - CVE-2022-1471 (GHSA-mjmj-j48q-9wg2): snakeyaml/1.31
  - CVE-2023-20863 (GHSA-wxqc-pxw9-g2p8): spring-core/5.3.26
  - CVE-2021-22573 (GHSA-xh97-72ww-2w58): google-oauth-client/1.27.0
- **Data Stories**
  - CVE-2023-30608: sqlparse/0.4.2, sqlparse/0.4.3
  - CVE-2023-3138: libx11/1.8.4-r0
  - CVE-2023-35945: nghttp2-libs/1.51.0-r0
  - CVE-2023-36053 (GHSA-jh3w-4vvf-mjgr): Django/4.2.1
  - CVE-2020-22218: libssh2-1/1.9.0-2
  - CVE-2022-42916: curl/7.74.0-1.3+deb11u7
  - CVE-2022-43551: curl/7.74.0-1.3+deb11u7
  - CVE-2023-1999: libwebp/1.2.4-r1
  - CVE-2023-23914: curl/7.74.0-1.3+deb11u7
  - CVE-2023-27533: libcurl4/7.74.0-1.3+deb11u7
  - CVE-2023-27534: curl/7.74.0-1.3+deb11u7
  - CVE-2023-28319: libcurl/7.88.1-r1

July 2023

Version 13.9.4

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking:

- CVE-2022-31690: spring-security-core/5.6.6
- CVE-2022-31692: spring-security-core/5.6.6
- CVE-2022-40152: woodstox-core/6.2.8
- CVE-2022-4450: libcrypto3/3.0.7-r2
- CVE-2023-0215: libssl3/3.0.7-r2
- CVE-2023-0216: libcrypto3/3.0.7-r2
- CVE-2023-0217: libssl3/3.0.7-r2
- CVE-2023-0286: libcrypto3/3.0.7-r2
- CVE-2023-0401: libssl3/3.0.7-r2
- CVE-2023-0464: libcrypto3/3.0.7-r2
- CVE-2023-20860: spring-core/5.3.21
- CVE-2023-24816: ipython/7.33.0
- CVE-2023-25652: git/2.38.4-r0
- CVE-2023-2650: libcrypto3/3.0.7-r2
- CVE-2023-27533: curl/7.87.0-r2
- CVE-2023-27534: curl/7.87.0-r2
- CVE-2023-28319: curl/7.87.0-r2
- CVE-2023-28531: openssh/9.1_p1-r2
- CVE-2023-28867: graphql-java/17.4
- CVE-2023-29007: git/2.38.4-r0
- CVE-2023-29491: ncurses-libs/6.3_p20221119-r0
- CVE-2023-2976: guava/29.0-jre
- CVE-2023-30535: snowflake-jdbc/3.13.14
- CVE-2023-34453: snappy-java/1.1.8.4
- CVE-2023-34454: snappy-java/1.1.8.4
- CVE-2023-34455: snappy-java/1.1.8.4
- CVE-2022-45688 (GHSA-3vqj-43w4-2q58): json/20140107
- CVE-2023-1370 (GHSA-493p-pfq6-5258): json-smart/2.4.7
- CVE-2023-30535 (GHSA-4g3j-c4wg-6j7x): snowflake-jdbc/3.13.14
- CVE-2022-1941 (GHSA-8gq9-2x98-w8hf): protobuf/3.20.1
- CVE-2022-34169 (GHSA-9339-86wc-4qgf): xalan/2.7.1
- CVE-2022-1471 (GHSA-mjmj-j48q-9wg2): snakeyaml/1.33
- CVE-2014-0107 (GHSA-rc2w-r4jq-7pfx): xalan/2.7.1
- CVE-2022-41723 (GHSA-vvpx-j8f3-3w6): golang.org/x/net/v0.6.0
- CVE-2023-0286 (GHSA-x4qr-2fvf-3mr5): cryptography/37.0.2

June 2023

Version 14.4.0

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking:

- CVE-2022-29458: libncursesw6/6.2+20201114-2
- CVE-2022-3515: gnupg-gpgconf/2.2.40-r0
- CVE-2022-3970: tiff/4.4.0-r1
- CVE-2023-0464: libcrypto3/3.0.8-r0
- CVE-2023-20860: spring-core/5.3.24
- CVE-2023-20862: spring-security-core/5.7.7
- CVE-2023-22743: git/2.38.4-r1
- CVE-2023-24329: python/3.10.10
- CVE-2023-2454: libpq-dev/13.9-0+deb11u1
- CVE-2023-25652: git/2.38.4-r1
- CVE-2023-28319: curl/7.88.1-r1
- CVE-2023-28531: openssh/9.1_p1-r2
- CVE-2023-28867: graphql-java/20.0
- CVE-2023-29007: git/2.38.4-r1
- CVE-2023-29491: ncurses-libs/6.3_p20221119-r0
- CVE-2023-24580 (GHSA-2hrw-hx67-34x6): Django/4.1.6
- CVE-2022-25857 (GHSA-3mc7-4q67-w48m): snakeyaml/1.30
- CVE-2023-30798 (GHSA-3qj8-93xh-pwh2): starlette/0.22.0
- CVE-2022-45688 (GHSA-3vqj-43w4-2q58): json/20140107
- CVE-2023-1370 (GHSA-493p-pfq6-5258): json-smart/2.4.8
- CVE-2023-34233 (GHSA-5w5m-pfw9-c8fp): snowflake-connector-python/3.0.1
- CVE-2022-1471 (GHSA-mjmj-j48q-9wg2): snakeyaml/1.33
- CVE-2023-31047 (GHSA-r3xc-prgr-mg9p): Django/4.1.6
- CVE-2022-41723 (GHSA-vvpx-j8f3-3w6h): golang.org/x/net/v0.6.0

MOVEit Application Breach

Ataccama does not use MOVEit for file transfer. Furthermore, the application does not exist in any Ataccama environment nor is it used in any part of Ataccama service provisioning.

April 2023

Version 14.3.0

- ONE-38485: Compression of HTTP communication was allowed for DPM and DPE, leaving them potentially vulnerable to BREACH attacks.
- ONE-41968: Active Directory service principal secret for Azure Data Lake Storage connections was visible to the admin user of DPM Admin Console.

View full list of fixed CVEs (the CVE name and reference, followed by the affected library) with high and above severity ranking:

- CVE-2015-20107: python/3.9.12
- CVE-2018-25032: python/3.9.12
- CVE-2018-8012: zookeeper/3.5.3-beta
- CVE-2019-8457: libdb5.3/5.3.28+dfsg1-0.8
- CVE-2020-10735: python/3.9.12
- CVE-2020-16156: perl-base/5.32.1-4+deb11u2
- CVE-2021-28165: etty-util-ajax/9.4.33.v20201020
- CVE-2021-28861: python/3.9.12
- CVE-2021-33560: libgcrypt20/1.8.7-6
- CVE-2021-41617: ssh/1:8.4p1-5+deb11u1
- CVE-2021-46848: libtasn1-6/4.16.0-2
- (CVE-2022-1304: libcom-err2/1.46.2-2
- CVE-2022-2048: jetty-util-ajax/9.4.33.v20201020
- CVE-2022-21698: github.com/prometheus/client_golang/v1.8.0
- CVE-2022-29458: libncurses6/6.2+20201114-2
- CVE-2022-34169: java/11.0.15+10
- CVE-2022-3509: protobuf-java/3.19.2
- CVE-2022-3510: protobuf-java/3.19.2
- CVE-2022-3715: bash/5.1-2+deb11u1
- CVE-2022-37454: python/3.9.12
- CVE-2022-42003: jackson-databind/2.13.4
- CVE-2022-42004: jackson-databind/2.13.3
- CVE-2022-42916: curl/7.74.0-1.3+deb11u5
- CVE-2022-42919: python/3.9.12
- CVE-2022-43551: curl/7.74.0-1.3+deb11u5
- CVE-2022-4450: libssl1.1/1.1.1n-0+deb11u3

- CVE-2022-44617: libxpm/3.5.14-r0
- CVE-2022-45061: python/3.9.12
- CVE-2022-46285: libxpm/3.5.14-r0
- CVE-2022-4883: libxpm/3.5.14-r0
- CVE-2022-4899: libzstd1/1.4.8+dfsg-2.1
- CVE-2023-0215: libssl1.1/1.1.1n-0+deb11u3
- CVE-2023-0216: libssl3/3.0.7-r2
- CVE-2023-0217: libssl3/3.0.7-r2
- CVE-2023-0286: libssl1.1/1.1.1f-1ubuntu2.13
- CVE-2023-0361: libgnutls30/3.7.1-5+deb11u2
- CVE-2023-20860: spring-core/5.3.25
- CVE-2023-23914: curl/7.74.0-1.3+deb11u5
- CVE-2023-24816: ipython/8.8.0
- CVE-2023-27533: curl/7.74.0-1.3+deb11u5
- CVE-2023-27534: curl/7.74.0-1.3+deb11u5
- CVE-2023-27535: curl/7.74.0-1.3+deb11u5
- CVE-2023-27536: curl/7.74.0-1.3+deb11u5
- CVE-2023-28867: graphql-java/18.3
- CVE-2023-29491: libncurses6/6.2+20201114-2
- CVE-2023-30535: snowflake-jdbc/3.13.23
- CVE-2023-24580 (GHSA-2hrw-hx67-34x6): Django/4.1.4
- CVE-2022-25857 (GHSA-3mc7-4q67-w48m): snakeyaml/1.30
- CVE-2023-30798 (GHSA-3qj8-93xh-pwh2): starlette/0.22.0
- CVE-2022-45688 (GHSA-3vqj-43w4-2q58): json/20220924
- CVE-2023-1370 (GHSA-493p-pfq6-5258): json-smart/2.4.8
- CVE-2023-30535 (GHSA-4g3j-c4wg-6j7x): snowflake-jdbc/3.13.23
- CVE-2020-1695 (GHSA-63cq-ppq8-cw6g): resteasy-client/3.9.3.Final
- CVE-2022-21698 (GHSA-cg3q-j54f-5p7p): github.com/prometheus/client_golang/v1.8.0
- CVE-2022-42003 (GHSA-jjjh-jjxp-wpff): jackson-databind/2.13.3
- CVE-2022-40898 (GHSA-qwmp-2cf2-g9g6): wheel/0.37.1
- CVE-2022-42004 (GHSA-rgv9-q543-rqg4): jackson-databind/2.13.3
- CVE-2023-27561 (GHSA-vpvm-3wq2-2wvm): github.com/opencontainers/runc/v1.1.0
- CVE-2023-0286 (GHSA-x4qr-2fvf-3mr5): cryptography/39.0.0

March 2023

Version 13.9.3

- CVE-2022-25168, CVE-2022-26612, CVE-2021-37404: Flaws in Apache Hadoop that could be exploited for arbitrary code execution or denial-of-service (DoS) attacks.
- CVE-2022-34169: A flaw in the Apache Xalan Java XSLT library that could be exploited to corrupt Java class files and execute arbitrary Java bytecode.
- CVE-2022-42003, CVE-2022-42004: Flaws in FasterXML jackson-databind (prior to version 2.14.0-rc1) allowing the use of deeply nested arrays, which can lead to resource exhaustion.
- CVE-2022-3509, CVE-2022-3510: Issues with parsing in textformat and 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) that can lead to a DoS attack.
- CVE-2022-46364: A server-side request forgery (SSRF) vulnerability in Apache CXF (prior to versions 3.5.5 and 3.4.10) allowing SSRF style attacks on web services with at least one parameter of any type.
- CVE-2020-10683: A flaw in dom4j (versions prior to 2.0.3 and 2.1.x to 2.1.2) that could allow XML code injection attacks and specifically XML external entity injection (XXE) attacks.
- CVE-2021-46848: An out-of-bounds read flaw in Libtasn1 (prior to version 4.19.0) that can result in an off-by-one error or memory corruption, or be exploited in a DoS attack.
- CVE-2019-8457: A flaw in SQLite3 (versions 3.6.0 through 3.27.2) that could result in a heap out-of-bound read when handling invalid rtree tables.
- CVE-2022-32221: A flaw in libcurl where the library might erroneously ask for data to send, which can in turn cause the application to misbehave and either send the wrong data or use memory after it was freed in a subsequent `POST` request.
- CVE-2022-42916, CVE-2022-43551: Flaws in curl (prior to version 7.86.0 and 7.87.0 respectively) allowing the HTTP Strict Transport Security (HSTS) check to be bypassed, which results in the library erroneously using HTTP instead of HTTPS.
- ONE-37804: A remote malicious user with `MMM_admin` role could execute commands on the DPE server by a specially crafted lookup file.

February 2023

Version 14.2.0

- CVE-2022-34169: A flaw in the Apache Xalan Java XSLT library that could be exploited to corrupt Java class files and execute arbitrary Java bytecode.
- CVE-2022-42003, CVE-2022-42004: Flaws in FasterXML jackson-databind (prior to version 2.14.0-rc1) allowing the use of deeply nested arrays, which can lead to resource exhaustion.
- CVE-2022-46364: A server-side request forgery (SSRF) vulnerability in Apache CXF (prior to versions 3.5.5 and 3.4.10) allowing SSRF style attacks on web services with at least one parameter of any type.

- CVE-2021-46848: An out-of-bounds read flaw in Libtasn1 (prior to version 4.19.0) that can result in an off-by-one error or memory corruption, or be exploited in a denial-of-service (DoS) attack.
- CVE-2022-3509, CVE-2022-3510: Issues with parsing in textformat and 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) that can lead to a DoS attack.
- ONE-37804: A remote malicious user with `MMM_admin` role could execute commands on the DPE server by a specially crafted lookup file.

January 2023

CVE-2022-23529

After a thorough investigation, we have determined that our production images and customer environments do not contain the vulnerability CVE-2022-23529 found in the node-jsonwebtoken library. This library was used in the development pipeline only and is not part of the final builds.

Version 14.1.0

- CVE-2021-23463, CVE-2022-23221 (DPM and DPE): Remote code execution flaw affecting H2 databases.
- CVE-2022-24823: Flaw in the `io.netty:netty-codec-http` package (versions earlier than 4.1.77) permitting local information disclosure through the local system temporary directory if file uploads are temporarily stored on the disk. Affects applications using Java 6 and earlier as well as code running on Unix-like systems and very old versions of Mac OSX and Windows.
- CVE-2022-25857: Flaw in `org.yaml:snakeyaml` (versions 0 through 1.30) allowing denial-of-service attacks.
- CVE-2022-31692: Flaw in Spring Security (versions 5.7 to 5.7.4 and 5.6 to 5.6.8) that could result in authorization rules getting bypassed using forward or include dispatcher types in the authorization filter.
- CVE-2020-10683, CVE-2018-1000632: Flaws in dom4j (versions prior to 2.0.3 and 2.1.x to 2.1.2, and versions prior to 2.1.1, respectively) that could allow XML code injection attacks and specifically XML external entity injection (XXE) attacks.

November 2022

Version 13.9.1

- CVE-2022-37734: Flaw in graphql-java (versions prior to 19.0) allowing denial-of-service attacks.
- CVE-2022-39135: Flaw in Apache Calcite (versions prior to 1.32.0) allowing potential XML External Entity (XXE) attacks due to several operators not restricting XML External Entity references in their configuration.
- CVE-2022-40023: Flaw in Sqlalchemy mako (versions prior to 1.2.2) allowing regular expression-based denial-of-service attacks when the Lexer class is used. Affects also babelplugin and linguaplugin.

- CVE-2022-1587: Out-of-bounds read flaw in the PCRE2 library. Affects also recursions in JIT-compiled regular expressions caused by duplicate data transfers.
- CVE-2021-3632: Flaw in Keycloak allowing anyone to register a new security device or key using the WebAuthn passwordless login flow in cases when no devices are registered for any user.
- CVE-2022-42889: Flaw in Apache Commons text (versions 1.5 through 1.9) allowing remote code execution or unintentional contact with remote servers.
- CVE-2022-1731: Flaw in Metasonic Doc WebClient where, if SSO or system authentication are enabled, the username field is open to SQL injection attacks.

CVE-2022-37786 and CVE-2022-3602

After learning about the OpenSSL vulnerability reported in late October 2022 (CVE-2022-37786 and CVE-2022-3602), we have performed a thorough analysis of our systems and applied the necessary patches as soon as they were released.

We can confirm that currently no Ataccama systems are affected by this vulnerability. Ataccama continues to monitor the environment and is prepared to address the situation immediately should anything change.

In case you have any further questions, contact the Ataccama Support team.

CVE-2022-39328, CVE-2022-39307, and CVE-2022-39306

We are aware of vulnerabilities (CVE-2022-39328, CVE-2022-39307, CVE-2022-39306) found in one of our third-party tools, Grafana. After investigation, we can confirm that the vulnerable version does not exist in on-premise deployments, Ataccama ONE PaaS, or ONE Portal.

October 2022

Apache Commons Text Vulnerability (CVE-2022-42889)

Ataccama products use the Apache Commons Text library but are not exposed to the vulnerability CVE-2022-42889 (affected versions 1.5 through 1.9).

Although the library is present in our software, there is no possibility for attack as the vulnerable class `StringSubstitutor` is not used. The same applies to the third-party software that Ataccama uses, namely Keycloak, MANTA, OpenSearch.

Starting from 12.10.0 and 13.9.1 releases, we have upgraded the Apache Commons Text library to version 1.10, which no longer contains the vulnerability. If upgrading is not an option at the moment, see Apache Commons Text Vulnerability (CVE-2022-42889) for more information about available workarounds.

For more detailed information about CVE-2022-42889, see:

- National Vulnerability Database entry on CVE-2022-42889
- Researchers Keep a Wary Eye on Critical New Vulnerability in Apache Commons Text

- Apache Commons Text Code Execution Flaws Disclosed, Exploit Available

August 2022

Version 13.9.0

- CVE-2022-31197: Flaw in the PostgreSQL JDBC Driver allowing Java programs (`java.sql.ResultRow.refreshRow()` function) to perform SQL injection attacks.
- CVE-2021-46828: Flaw in libtirpc allowing to trigger an infinite loop where no new TCP connections are accepted.
- CVE-2022-32207: Flaw in cURL related to accidental permission changes when cookies and specific header data are saved to local files.
- CVE-2022-31107, CVE-2022-31097: Flaws in Grafana allowing a user authenticated through OAuth to overtake another user's account or to grant themselves higher permissions (from editor to admin).
- CVE-2022-2048: Flaw in Eclipse Jetty HTTP/2 server that could lead to denial-of-service attacks following an invalid HTTP/2 request.
- CVE-2022-25236: Flaw in expat (libexpat) that could result in arbitrary code execution.

July 2022

Version 13.7.x

- CVE-2021-37136, CVE-2021-37137: Flaws in two decoder functions that can lead to excessive memory usage and DoS attacks in the `netty-codec` used by Java.
- CVE-2021-43858, CVE-2021-21287, CVE-2020-11012: Authentication bypass issues in MinIO.
- CVE-2021-22569, CVE-2021-22570: Issues related to parsing in `protobuf-java`.
- CVE-2021-44228, CVE-2021-45046: Arbitrary code execution flaw in `log4j-core`.
- CVE-2019-20445: Flaw related to `Content-Length` header in Netty.

Version 13.8.x

- CVE-2021-43527: Remote code execution flaw related to NSS verification of certificates. Affects Ubuntu 18.04 OS.
- CVE-2022-0778: Flaw in OpenSSL allowing to trigger an infinite loop. Affects Ubuntu 18.04 OS.
- CVE-2022-25235: Flaw in `expat` that could result in arbitrary code execution. Affects Ubuntu 18.04 OS.
- CVE-2021-33910: Flaw in `systemd` potentially impacting system availability. Affects Ubuntu 18.04 OS.
- CVE-2022-24407: Arbitrary code execution flaw in Debian-based OS due to improper SQL input validation.
- CVE-2022-25315: Flaw in Debian-based OS that can result in a DoS attack or arbitrary code

execution.

- CVE-2021-23463, CVE-2022-23221 (MDM Server), CVE-2021-42392: Remote code execution flaws affecting H2 databases.

Apache Commons Text Vulnerability (CVE-2022-42889)

The following article describes how to remove the Apache Commons Text library in versions earlier than 12.10.0 or 13.9.1, depending on whether you are using Ataccama ONE Platform or Ataccama ONE Gen2 Platform respectively.

Overview

Ataccama products use the Apache Commons Text library but are not exposed to the vulnerability CVE-2022-42889 (affected versions 1.5 through 1.9). Although the library is present in our software, there is no possibility for attack as the vulnerable class `StringSubstitutor` is not used. The same applies to the third-party software that Ataccama uses, namely Keycloak, MANTA, OpenSearch.

Starting from 12.10.0 and 13.9.1 releases, we have upgraded the Apache Commons Text library to version 1.10, which no longer contains the vulnerability.

To remove the affected library from your instance, follow the instructions for your product version.

Version 13.x (13.9.0 and earlier)

The Apache Commons Text library should be removed from the following modules: ONE Desktop, Data Processing Engine (DPE), ONE Runtime Server.

As the affected library was introduced to Ataccama products indirectly through the Salesforce connector and its libraries, choose one of the following options depending on whether you are using Salesforce data sources or not.

Keep in mind the following:

- The file versions might differ based on the specific 13.x version that you are using.
- The application must not be running while you perform the upgrade.

If you are not using the Salesforce connector

If you are not using Salesforce data sources, delete the following files and folders:

- **ONE Desktop**:
  - `$DESKTOP/runtime/lib/commons-text-1.9.jar`
  - `$DESKTOP/plugins/com.ataccama.extension.salesforce.ide.ui_13.9.1.jar`
- **Data Processing Engine (DPE)**
  - `/opt/ataccama/one/dpe/lib/runtime/commons-text-1.9.jar`
  - `/opt/ataccama/one/dpe/plugin/salesforce-datasource-dpe-13.4.3.zip`

- The entire directory `/opt/ataccama/one/dpe/plugin/salesforce-datasource-dpe-13.4.3`
- **ONE Runtime Server**
  - `runtime/lib/commons-text-1.9.jar`

If you are using the Salesforce connector

If you cannot upgrade and are using Salesforce data sources, do the following:

1. Download the patched `library commons-text-1.10.jar` from the Apache Commons website.
2. **In Data Processing Engine (DPE)**:
   a. Replace the library `commons-text-1.9.jar` with `commons-text-1.10.jar` in the following locations:
      - `/opt/ataccama/one/dpe/lib/runtime`
      - In the archive `/opt/ataccama/one/dpe/plugin/salesforce-datasource-dpe-13.4.3.zip`
   b. Delete the entire folder: `/opt/ataccama/one/dpe/plugin/salesforce-datasource-dpe-13.4.3`. This way, the updated plugin archive will be automatically extracted once you start the application again.
3. In ONE Runtime Server, replace the library `commons-text-1.9.jar` with `commons-text-1.10.jar` in `runtime/lib`.
4. If you are using Salesforce in ONE Desktop, reach out to Ataccama Support for further assistance.

Installations using OpenSearch

Upgrade OpenSearch to version 1.3.7.

Version 12.x (12.9.0 and earlier)

The Apache Commons Text library should be replaced in ONE Web Application using the following steps.

Keep in mind the following:

- The file version might differ based on the specific 12.x version that you are using.
- The application must not be running while you perform the upgrade.
  1. Download the patched library `commons-text-1.10.jar` from the Apache Commons website.
  2. Replace the library `commons-text-1.6.jar` with `commons-text-1.10.jar` in the following location: `Ataccama/one/webapps/ROOT/WEB-INF/lib`.