# Teradata® Vantage 2.0 Release Summary

Deployment Platforms: Teradata Vantage on AWS
Teradata Vantage on Azure

June 2020

B700-4000-060C
DOCS.TERADATA.COM

## Copyright and Trademarks



## Product Safety

| Safety type | Description |
|---|---|
| *NOTICE* | Indicates a situation which, if not avoided, could result in damage to property, such as to equipment or data, but not related to personal injury. |
| CAUTION | Indicates a hazardous situation which, if not avoided, could result in minor or moderate personal injury. |
| WARNING | Indicates a hazardous situation which, if not avoided, could result in death or serious personal injury. |

## Warranty Disclaimer

**Except as may be provided in a separate written agreement with Teradata or required by applicable law, the information contained in this document is provided on an "as-is" basis, without warranty of any kind, either express or implied, including the implied warranties of merchantability, fitness for a particular purpose, or noninfringement.**

The information contained in this document may contain references or cross-references to features, functions, products, or services that are not announced or available in your country. Such references do not imply that Teradata Corporation intends to announce such features, functions, products, or services in your country. Please consult your local Teradata Corporation representative for those features, functions, products, or services available in your country.

The information contained in this document may be changed or updated by Teradata at any time without notice. Teradata may also make changes in the products or services described in this information at any time without notice.

## Feedback

To maintain the quality of our products and services, email your comments on the accuracy, clarity, organization, and value of this document to: docs@teradata.com.

Any comments or materials (collectively referred to as "Feedback") sent to Teradata Corporation will be deemed nonconfidential. Without any payment or other obligation of any kind and without any restriction of any kind, Teradata and its affiliates are hereby free to (1) reproduce, distribute, provide access to, publish, transmit, publicly display, publicly perform, and create derivative works of, the Feedback, (2) use any ideas, concepts, know-how, and techniques contained in such Feedback for any purpose whatsoever, including developing, manufacturing, and marketing products and services incorporating the Feedback, and (3) authorize others to do any or all of the above.

Teradata Vantage™ is our flagship analytic platform offering, which evolved from our industry-leading Teradata® Database. Until references in content are updated to reflect this change, the term Teradata Database is synonymous with Teradata Vantage.

Advanced SQL Engine (was NewSQL Engine) is a core capability of Teradata Vantage, based on our best-in-class Teradata Database. Advanced SQL refers to the ability to run advanced analytic functions beyond that of standard SQL.

The following lists the fixed and known issues in this release. If you experience any of the following issues, open an incident with Teradata Customer Support and include the Reference ID in your description.

## Compatibility Matrix

For component compatibility information:

1. Go to support.teradata.com
2. Login
3. Search for KB0012513

## Key Features

The Vantage 2.0 release contains a major update to the Advanced SQL Engine that enables customers to natively access storage from AWS S3 and Azure Blob. As companies continue to adopt object storage for modern data lakes, this Native Object Store (NOS) READ capability allows you to seamlessly access that data where it lives.

This release can be deployed as-a-service on AWS and Azure. Refer to Vantage 2.0 documentation for further details.

## Fixed Issues

### Data Stream Architecture (DSA)

| Reference ID | Description |
|---|---|
| DSA-21416 | **Description**: Spring Boot Antlib is a Spring library used to build our DSA REST project. Spring Boot Antlib 1.5.9.RELEASE contained the following security vulnerabilities:  Spring Data Commons is vulnerable to remote code execution (*RCE*) due to improper neutralization of special elements when dealing with certain requests. The attackers could leverage this flaw to run arbitrary code on the target system using multiple attack vectors.; CVSS Overall Base Score: 7.5<br>**Workaround**: The DSA REST project was removed Spring Boot Antlib starting from DSA 17.00.01.00. The DSA REST service is also something not externally supported currently. Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed o Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. 2. The DSA REST service's status is viewable by executing "/etc/init.d/dsc status". This can notify the user if this application has gone down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |

| | |
|---|---|
| DSA-20928 | **Description**: Xerces-C++ is a validating XML parser written in a portable subset of C++. Xerces-C++ makes it easy to give your application the ability to read and write XML data. A shared library is provided for parsing, generating, manipulating, and validating XML documents using the DOM, SAX, and SAX2 APIs. Apache Xerces C++ XML Parser 3.1.1 contained the following security vulnerabilities: - CVE-2016-2099): Use-after-free vulnerability in validators/DTD/DTDScanner.cpp in Apache Xerces C++ 3.1.3 and earlier allows context-dependent attackers to have unspecified impact via an invalid character in an XML document. CWE-416: Use After Free; CVSS Overall Base Score: 10 - CVE-2017-12627 : In Apache Xerces-C XML Parser library before 3.2.1, processing of external DTD paths can result in a null pointer dereference under certain conditions.; CVSS Overall Base Score: 7.5 - CVE-201 0729: Multiple buffer overflows in (1) internal/XMLReader.cpp, (2) util/XMLURL.cpp, and (3) util/XMLUri.cpp in the XML Parser library in Apache Xerces-C before 3.1.3 allow remote attackers to cause a denial of service (segmentation fault or memory corruption) or possibly execute arbitrary code via a crafted document.; CVSS Overall Base Score: 7.5 - CVE-2018-1311: The Apache Xerces-C 3.0.0 to 3.2.2 XML parser contains a use-after-free error triggered during the scanning of external DTDs. This flaw has not been addressed in the maintained version of the library and has no current mitigation other than to disable DTD processing. This can be accomplished via the DOM using a standard parser feature, or via SAX using the XERCES_DISABLE_DTD environment variable.; CVSS Overall Base Score: 6.8 - CVE-2015-0252: internal/XMLReader.cpp in Apache Xerces-C before 3.1.2 allows remote attackers to cause a denial of service (segmentation fault and crash) via crafted XML data.; CVSS Overall Base Score: 5 - CVE-2016-4463: Stack-based buffer overflow in Apache Xerces-C++ before 3.1.4 allows context-dependent attackers to cause a denial of service via a deeply nested DTD.; CVSS Overall Base Score: 5<br>**Workaround**: The BarNC project was upgraded to use Xerces C++ XML Parser 3.2.2 starting from DSA 17.00.00.00. Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed on Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. 2. The BarNC process' status is viewable by executing "/etc/init.d/clienthandler status". This can notify the user if this application has gone down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |

| | |
|---|---|
| DSA-20794 | **Description**: jackson-databind is a General data-binding package for Jackson (2.x): works on streaming API (core) implementation(s). jackson-databind 2.9.10 contained the following security vulnerabilities: - CVE-2020-8840: FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.; CVSS Overall Base Score: 7.5 - CVE-2020-9546 ): FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config).; CVSS Overall Base Score: 6.8 - CVE-2020-9547: FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.ibatis.sqlmap.engine.transaction.jta.JtaTransactionConfig (aka ibatis-sqlmap).; CVSS Overall Base Score: 6.8 - CVE-2020-9548: FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPConfig (aka anteros-core). - CVE-2020-10672: FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal.XaPooledConnectionFactory (aka aries.transaction.jms).; CVSS Overall Base Score: 6.8 - CVE-2020-10673: FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.caucho.config.types.ResourceRef (aka caucho-quercus).; CVSS Overall Base Score: 6.8 - CVE-2019-17531: A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.; CVSS Overall Base Score: 7.5 - CVE-2019-20330: FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.; CVSS Overall Base Score: 7.5 - CVE-2019-16943: A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataSource mishandling.; CVSS Overall Base Score: 7.5 - CVE-2019-16942: A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the commons-dbcp (1.4) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of org.apache.commons.dbcp.datasources.SharedPoolDataSource and org.apache.commons.dbcp.datasources.PerUserPoolDataSource mishandling.; CVSS Overall Base Score: 7.5<br><br>**Workaround**: The DSA REST project was upgraded to use jackson-databind 2.10.1 starting from DSA 17.00.00.00. The DSA REST service is also something not externally supported currently. Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed on Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. 2. The DSA REST service's status is viewable by executing "/etc/init.d/dsc status". This can notify the user if this application has gone down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |

## Server Management Software

| Reference ID | Description |
|---|---|
| SM-29725 | Update of Netty |
| SM-29354 | Updating Spring Framework to resolve CVE-2020-5398<br>**Workaround**: CMIC is a closed system and does not allow outside software to run on it. External access to the host OS is very controlled to specific IP addresses/users.<br>**Deployments**: All |
| SM-28655 | Update Apache log4j for CVE-2019-17571<br>**Workaround**: CMIC is a closed system and does not allow outside software to run on it. External access to the host OS is very controlled to specific IP addresses/users.<br>**Apache workaround**: https://nsfocusglobal.com/apache-log4j-deserialization-remote-code-execution-cve-2019-17571-vulnerability-threat-alert/<br>**Deployments**: All |

## Advanced SQL Engine

| Reference ID | Description |
|---|---|
| SQLE-513 | **Description**:<br><br>**---- OPNDPE Fixed Issues ----**<br>DR 193091 Priority 2<br>System debugger is getting SEGV after issuing a kill command when the program is in initial stage(before unwind information is not constructed for the thread).<br>DR 193726 Priority 2<br>Cnstool shows 6: then 5: with vprocmanager output leaving screen 5 waiting for a command to enter and when Plan Cache sends it, it no longer works even afterproviding "ok" input from cnswindow 5.<br>DR 193867 Priority 3<br><br>To test tpasuspend/resume feature wrote few feature test cases. In this DR added few enhancements to these test cases.<br>- Add invalid input option for the test runs.<br>- Instead of sleeping 300 seconds to bring the database up when test given a restart change test to wait until dbs is up or timeout after 10 mins.<br>- Run tests when the ssytem is in RUN/STARTED. state only (Ealier we are not running tests when PDE is in DOWN/HARDSTOP state)<br>DR 193904 Priority 2<br>fsgagestat -z getting failed while reading fsg_waitforcache symbol.<br>DR 193927 Priority 3<br>To promote tpasuspend test cases to PTE server masterscript.pl is not allowing to run interactive mode .So need to change the suspend test cases from interactive to execute all he tests.<br><br>TVSA:<br><br>DR 193722 Priority 2<br>RUDEMIGRATOR_MIGRATOR_TYPE_INVALID exception with a stack backtrace appearsin /var/log/messages. No restart or other bad behavior results<br><br>**PTBMS Fixed Issues**<br><br>DR 193459 Priority 2<br>While executing the query on Recoverable network protocol with KeepResp on configuration box if the query aborted may lead to segv due to the leftover ReqCtx.<br>DR 193553 Priority 2<br>SpoolCacheThr does not honor when intermediate spool being referenced across the AMP steps.<br>DR 193639 Priority 2<br>Symptoms noticed by the customer included signs of data skew for AUTOTEMP tables: certain amps had higher levels of PERM space. We used Ferret scoped to a specific<br>AUTOTEMP table with the "showwhere" command: those AMPs suspected of being stuck also showed much higher numbers of cylinders holding COLD data, not yet compressed. |

Customer enabled ATC Debug mode to help diagnose suspected stuck AMPs:

ATC debug mode at customer site hit DR 193660

# dbscontrol
> mo int 8 0 = 400 <-- FILTRACEAUTOTEMPCOMP
> write/quit

Darts won't allow more than a few lines in this section. Attaching ATC Debug/trace
output from AMP-10 showing dictionary table hibernation loop.
DR 193660 Priority 2
After enabled ATC traces as follows:
mo int 8 0 = 400

We see that the debug traces written to ATC debug file for FSUTRACKSPACE module have (null) for databasename and other entries are garbage.

For Example:

Wed Feb 5 17:27:12 2020
FSUTRACKSPACE
Database space committed for Database (null) (03F1 0000)
Tableid.uniq: 088E 53010014
Deltabytes: 1342198528
WTJDeltabytes: 1090537728
DR 193750 Priority 2
Fastpath partition delete on Columnar table inflates table if online archive logging is active.
DR 193753 Priority 2
QGLimit throttle does not work for function aliases on coprocessor
DR 193754 Priority 2
Drop Role places table write lock on DBC.SessionTbl, it can cause deadlock with logon operation.

DR 193805 Priority 2
Select on view/macro with NPATH and it's inner-subquery field referred with alias reports error.
DR 193809 Priority 2
AnalyzeSP gets out of spool error due to non-optimal plans
DR 193828 Priority 2
The replication groups get put into a bad state which can not be resettled until the DBS under goes a tpareset. This would put CDM out of commission in a
Unity environment until the tpareset occurs.
DR 193832 Priority 2
Abort logoff using the syslib.Abortsession() api can cause restart with 3200
DR 193837 Priority 2
Logging online archive is not turned on if it's retried with DR 193087 fix.
DR 193841 Priority 2

| | |
|---|---|
| | Customer is seeing negative spool values through query monitor in Viewpoint.<br>Note: When the AMPSpoolUsage value exceeds ?9223372036854775807?.<br>DR 193848 Priority 2<br>3610 may happen for query with Union when index is picked and there is concurrent session creating new index.<br>DR 193864 Priority 2<br><br>Merge_Into sql failed with Failure 3812 The positional assignment list has too few values for non select * case for valid select list and insert values.<br>select list : select td_timecode, c1, td_timebucket from mrg_src_nb_ns<br><br>Insert values: src.td_timecode, src.c1, src.td_timebucket<br>DR 193868 Priority 2<br>Parser may fail with SEGV when multiple join indexes are involved.<br>DR 193880 Priority 2<br>Missing change data due to normal priority Work Queue Flow Control event got overwritten<br><br>DR 193882 Priority 2<br>5273 restart or failure may happen for query using 1MB Spool Rows and Number data types.<br>DR 193885 Priority 1<br>CUSTOMER-PROBLEM-DESCRIPTION:<br>Outputs are different when MCD is enabled (vs disabled) on query<br>with pack function.<br>DR 193889 Priority 2<br>CREATE/REPLACE PROCEDURE will fail with 5601 error when double quotes used in the<br>EXTERNAL NAME clause.<br>DR 193898 Priority 1<br>Query with below semantics can give wrong results.<br><br>1. Multi value compression<br>2. Condition on compression field along with other fields<br>3. The other fields are defined after the compressed column.<br>DR 193902 Priority 2<br>some SATTC feature may not work.<br>DR 193911 Priority 2<br>We are observing incorrect results with queries containing <= & >= filtering<br>condition on a parquet table.<br>DR 193916 Priority 2<br>Whenever DBQL Logging is turned on and User tries to run READ_NOS query providing ACCESS_KEY in the NVPs then the ACCESS_KEY value is not being hidden in DBQL Query text.<br><br>**Workaround**: N/A<br>**Deployments**: AWS, Azure |

### Teradata Viewpoint

| Reference ID | Description |
|---|---|
| VP-50533 | **Description**: The repeated creation of the classes causes JDK 8 to eventually run out of memory. Depending on the number of systems monitored, the session monitor rate, and the number of sessions, this leak will accrue more or less slowly.<br>**Workaround**: None.<br>**Deployments**: All |

## Known Issues

### Data Stream Architecture (DSA)

| Reference ID | Description |
|---|---|
| DSA-22112 | **Description**: The Spring Framework is an application framework and inversion of control container for the Java platform. The Spring libraries 3.2.2 and 4.3.13.RELEASE contained the following security vulnerabilities: - BDSA-2018-1076: Spring Data Commons is vulnerable to remote code execution (*RCE*) due to improper neutralization of special elements when dealing with certain requests. The attackers could leverage this flaw to run arbitrary code on the target system using multiple attack vectors.; CVSS Overall Base Score: 7.5<br>**Workaround**: Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed on Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |

| | |
|---|---|
| DSA-21414 | **Description**: Apache log4j is a Java-based logging utility. Apache log4j 1.2.14 and 1.2.17 contained the following security vulnerabilities: - BDSA-2017-0180: A deserialization flaw in log4j can lead to remote arbitrary code execution.; CVSS Overall Base Score: 7.5<br>**Workaround**: Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed on Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |
| DSA-20788 | **Description** (same as DSA-22112): The Spring Framework is an application framework and inversion of control container for the Java platform. The Spring libraries 3.2.2 and 4.3.13.RELEASE contained the following security vulnerabilities: - BDSA-2018-1076: Spring Data Commons is vulnerable to remote code execution (*RCE*) due to improper neutralization of special elements when dealing with certain requests. The attackers could leverage this flaw to run arbitrary code on the target system using multiple attack vectors.; CVSS Overall Base Score: 7.5<br>**Workaround**: Preventative Controls: The scale of impact is reduced because there are several mitigating controls in place, such as: 1. The user needs access to internal network. 2. The client device/server needs to have BARCmdline package installed or the barportlets package installed on Viewpoint to gain access to the DSC service. 3. In addition, Viewpoint User Authentication requires Viewpoint credentials to execute BARCmdline commands. 4. https protocol is available for DSA REST service. A valid CA certificate is required to invoke different endpoints of this service. 5. SSL connection type is also supported for ActiveMQ, which is the Message Queue the different DSA components use to communicate with one another. Detective Controls: 1. Unsuccessful attempts to exploit the vulnerabilities can cause the system to crash, prompting an alert when the particular system is down. Corrective Controls: 1. Disaster Recovery of DSC is available. If there is persistent code, etc. in the DSA projects, the user has an ability to wipe out their entire DSA environments and perform a fresh install using different passwords/credentials. Afterwards, the user can restore back the Repository data back to the state that they wish to revert back to. Compensatory Controls: 1. The attacker will need access to the Teradata Database in order to access/read data. Through DSA, the user can potentially see the database object names and types, but not the row data. 2. The credentials, etc. within the Job Plan sent over to the Teradata Database are encrypted. The data sent over to the different storage devices is encrypted as well.<br>**Deployments**: All |

## Advanced SQL Engine

| Reference ID | Description |
|---|---|
| SQLE-511 | **Description:** 3707 Syntax error, expected something like ')' between a string or a Unicode character literal and 's'.<br>**Workaround** - For 194127 disable nested join "diagnostic nonestedjoin". For 194141, do not include quotes in partitioning expression.<br>**Deployments** - AWS/Azure |

## DBSQ

| Reference ID | Description |
|---|---|
| DBSQ-3762 | **Description**: Error messages show old, nonstandardized argument and table names.<br>**Workaround**: For old names that appear in error messages and their corresponding new names, see Teradata Vantage™ Machine Learning Engine Analytic Function Reference, B700-4003. |

## Teradata Viewpoint

| Reference ID | Description |
|---|---|
| VP-50971 | **Description**: Disable the creation of primary keys in a non-clustered environment to avoid locking postgres tables<br>**Workaround**: Apply Knowledge article KB0032483 to disable creating the Primary Key.<br>**Deployments**: All |
| VP-50858 | **Description**: Upgrade to Tomcat 9.0.31 to address the following high (CVSS >=7.0) security risks: * CVE-2020-1938 * CVE-2020-1935 (not yet rated)<br>**Workaround**: N/A Ease of exploitation: * CVE-2020-1938: This only affects the AJP protocol connector which we do not use and do not have enabled. It is a serious vulnerability, but not for Viewpoint. * CVE-2020-1935: Very difficult. From the CVE, "a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely."<br>**Deployments**: All |