Teradata® Vantage 1.1.2 Release Summary

Deployment Platform: Teradata IntelliFlex™

March 2020

B700-4000-030C
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.

Fixed Issues

Machine Learning Engine

Reference ID	Description
MLE-4790	This upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2019-3855 It should also address the following medium security risks: * CVE-2016-0787 * CVE-2019-13115 * CVE-2019-17498 * CVE-2019-3859 * CVE-2019-3862 * CVE-2019-3858 * CVE-2019-3860 * CVE-2019-3861 * CVE-2019-3856 * CVE-2019-3863 * CVE-2015-1782 * CVE-2019-3857

Teradata QueryGrid

Reference ID	Description
QUERYGRID-11435	In QGM Portlet - Unable to see the active tdqg-manager-1 instance.

Teradata Viewpoint

Reference ID	Description
VP-50366	**Description**: The Apache CXF upgrade should address the following high (CVSS >=7.0) security risk: * CVE-2019-12419 (BDSA-2019-3418). **Workaround**: N/A
VP-50159	**Description**: The Jetspeed-2 Enterprise Portal 2.1.4 to 2.3.1 upgrade should address the following high (CVSS >=7.0) security risk: * CVE-2016-0710 * CVE-2016-0709 **Workaround**: N/A
VP-50157	**Description**: The jackson-databind 2.9.9 to 2.10 upgrade should address the following high (CVSS >=7.0) security risk: * CVE-2019-14540 (BDSA-2019-2980) * CVE-2019-16943 (BDSA-2019-3135) * CVE-2019-17267 (BDSA-2019-3151) * CVE-2019-16942 (BDSA-2019-3136) * CVE-2019-14379 (BDSA-2019-2355) * CVE-2019-16335 (BDSA-2019-2978) **Workaround**: N/A
VP-50156	**Description**: The Upgrade Bouncy Castle 1.51 to 1.64 upgrade should address the following high (CVSS >=7.0) security risk: * CVE-2018-1000613 (BDSA-2018-2512) **Workaround**: N/A
VP-50155	**Description**: The Apache Commons Beanutils 1.9.2 to 1.9.4 upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2019-10086 (BDSA-2014-0129) **Workaround**: N/A **Deployments**: All
VP-50154	**Description**: The Scala to 2.11.12 upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2017-15288 (BDSA-2017-1963) **Workaround**: N/A **Deployments**: All

VP-49825	**Description**: Remove dependency on `td-commons`(CVSS >=7.0) security risks: * BDSA-2015-0110 **Workaround**: N/A **Deployments**: All
VP-49823	**Description**: The X-Stream library upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2013-7285 (BDSA-2013-0046) * CVE-2019-10173 (BDSA-2018-5035) **Workaround**: N/A **Deployments**: All
VP-49261	**Description**: The update of Postgres configuration should address the following high (CVSS >=7.0) security risks: * CVE-2018-1058 **Workaround**: N/A **Deployments**: All
VP-49260	**Description**: The Postgres upgrade to 9.4.19 should address the following high (CVSS >=7.0) security risks: * CVE-2018-10915 * CVE-2018-10925 **Workaround**: N/A **Deployments**: All
VP-47836	**Description**: The Commons Collections library upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2017-15708 **Workaround**: N/A **Deployments**: All
VP-47568	**Description**: The Apache Tomcat 9.0.19 upgrade should address the following high (CVSS >=7.0) security risks: * CVE-2016-3092 * CVE-2016-8735 (BDSA-2016-0064) * CVE-2018-1304 * CVE-2018-1305 * CVE-2018-1305 * CVE-2018-8014 (BDSA-2018-1521) * CVE-2019-0232 (BDSA-2019-1146) **Workaround**: N/A **Deployments**: All

Known Issues

Teradata 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 **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. **Deployments**: All

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: - 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 **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 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. **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 **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. **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 (BDSA-2016-0203): 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 (BDSA-2018-0621): 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-2016-0729 (BDSA-2016-0024): 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 (BDSA-2019-4014): 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 **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. **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 (BDSA-2020-0252): 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 (BDSA-2020-0363): 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 (BDSA-2020-0361): 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 (BDSA-2020-0354): 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 (BDSA-2020-0486): 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 (BDSA-2020-0487): 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 (BDSA-2019-3215): 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 (BDSA-2019-4111): 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 (BDSA-2019-3135): 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 (BDSA-2019-3136): 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 **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. **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 **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. **Deployments**: All

Machine Learning Engine

Reference ID	Description
MLE-5823	**Description**: CVE-2019-0211 In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **Workaround**: None. Upgrade httpd to 2.4.41. **Deployment**: All
MLE-5822	**Description**: Threat record: CVE-2019-17571: https://nvd.nist.gov/vuln/detail/CVE-2019-17571 " Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17. " **Workaround**: Workaround provided by Apache: https://nsfocusglobal.com/apache-log4j-deserialization-remote-code-execution-cve-2019-17571-vulnerability-threat-alert/ " If users cannot upgrade to V2.8.2 or later for the time being, they can also prevent the socket port enabled by the SocketServer class in Log4j from being opened to the public network. " Since we do not expose socket port from this container to any public network (cluster is generally locked down), we should be fine with this issue for now. **Deployment** (affected platforms) All
MLE-5800	**Description**: During Black Duck scans, GCC and Python-devel package was found to be a security vulnerability. Hence it was needed to remove those from upgrade images. Deployment (platform impacted) Due to removal of those packages, Azure platform will be impacted. There is no impact on IFX/AWS. **Workaround** As a workaround, Azure upgrades would be to manually collect all MLE UDFs from old MLE and install them in the new MLE. **Deployment**: All
MLE-5120	**Description**: CVE-2013-1900: PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, and 8.4.x before 8.4.17, when using OpenSSL, generates insufficiently random numbers, which might allow remote authenticated users to have an unspecified impact via vectors related to the "contrib/pgcrypto functions". Other medium and low security risks which are related to above issue are CVE-2014-0060, CVE-2014-0066, CVE-2015-3165, CVE-2016-5424, CVE-2014-0067,CVE-2014-0062, CVE-2012-3488, CVE-2015-3167, CVE-2016-0773, CVE-2016-0768, CVE-2017-7484, CVE-2017-7486, CVE-2015-5289, CVE-2015-5288, CVE-2018-1115,CVE-2014-0063, CVE-2014-0065, CVE-2014-0064, CVE-2014-0061, CVE-2016-5423, CVE-2013-0255 and CVE-2017-14798. **Workaround**: Exploitation of PostgreSQL security issue can be Mitigated by network segmentation and firewall rules.There is no direct customer access to PostgreSQL rendering security issues unexploitable. **Deployment**: All
MLE-3997	**Description**: CVE-2013-0252: boost::locale::utf::utf_traits in the Boost.Locale library in Boost 1.48 through 1.52 does not properly detect certain invalid UTF-8 sequences, which might allow remote attackers to bypass input validation protection mechanisms via crafted trailing bytes. **Workaround**: Existing security issues in boost library are not exploitable due to the requirement of local access required within MLE services. There is no direct customer access to the Operating System and/or Containers rendering security issues unexploited. **Deployment**: All

MLE-3649	**Description**: CVE-2016-9013: Django 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3 use a hardcoded password for a temporary database user created when running tests with an Oracle database, which makes it easier for remote attackers to obtain access to the database server by leveraging failure to manually specify a password in the database settings TEST dictionary. In MLE, This CVE is not applicable as MLE does not use Oracle. **Workaround**: Not applicable. **Deployment**: None. This CVE is not applicable for MLE **Description**: CVE-2014-0474: The (1) FilePathField, (2) GenericIPAddressField, and (3) IPAddressField model field classes in Django before 1.4.11, 1.5.x before 1.5.6, 1.6.x before 1.6.3, and 1.7.x before 1.7 beta 2 do not properly perform type conversion, which allows remote attackers to have unspecified impact and vectors, related to "MySQL typecasting." **Workaround**: Not applicable. **Deployment**: None. This CVE is not applicable for MLE **Description**: CVE-2015-5143: The session backends in Django before 1.4.21, 1.5.x through 1.6.x, 1.7.x before 1.7.9, and 1.8.x before 1.8.3 allows remote attackers to cause a denial of service (session store consumption) via multiple requests with unique session keys. **Workaround**: None. Upgrade Django to latest version (1.11.x) **Deployment**: All
MLE-3540	**Description**: CVE-2016-1234: Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.7, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name. Other issues that are related to above and glibc are CVE-2014-9402, CVE-2015-8779, CVE-2014-9761, CVE-2018-6485, CVE-2018-11236, CVE-2019-9169, CVE-2017-15670, CVE-2015-1472, CVE-2010-0015, CVE-2014-4043, CVE-2012-4412, CVE-2015-8778, CVE-2017-15804, CVE-2014-9984, CVE-2010-3856, CVE-2018-1000001, CVE-2010-0296, CVE-2017-1000366, CVE-2015-5277 **Workaround**: Existing security issues in glibc are not exploitable due to the requirement of local access required within MLE services. There is no direct customer access to the Operating System and/or Containers rendering security issues unexploitable. **Platforms impacted**: All
MLE-3491	**Description**: The MLE connector stats handler thread continues to use old connector password after it is changed. Workaround: Contact Teradata Customer Support for assistance. **Deployments**: All
MLE-3405	**Description**: ML Engine does not support QueryGrid link names that contain whitespace. **Workaround**: The administrator should not use whitespace in names when they create links between the ML engine and other components. Doing so causes an error in the Failure Detection and Restart capability of the ML engine. **Deployment**: All
MLE-3031	**Description**: Some rows in ML Engine stats table may contain empty stats. **Workaround**: None. The rows with empty stats may be confusing, but do not affect anything. **Deployments**: All
MLE-2220	**Description**: PERM space size of Query Level Monitoring (QLM) database is created with 10 Mb for each AMP. PERM space is full if QLM queries fail with [ERROR]: No more room in database td_mle_db. **Workaround**: None **Deployments**: All
MLE-1392	**Description**: Stored procedures in pm database, such as pm.install_afile, fail if first master node in analytic cluster is unavailable. **Workaround**: Administrator must log into each TPA node using ssh, then change the file /home/tdatuser/.ssh/ config to point to another node in **Deployment**: All analytic cluster.

Machine Learning Engine Analytic Functions

Reference ID	Description
ANLY-10226	**Issue**: For XGBoost function, if sparse format is used for input dataset, the function may fail. **Workaround**: Add uniqueID() argument when sparse format is used in XGBoost function
ANLY-10087	Backward incompatibility caused by making AttributeValueColumn required. Being optional as it was before made no sense as it was defaulted to value 1 for all the attributes.
ANLY-8534	**Description**: This is a new function that wraps the previous NaiveBayesMap and NaiveBayesReduce functions. We advise to use this function as it has a simpler syntax and other improvements. However, the previous nested syntax is still supported. **Deployments**: All.
ANLY-8328	The StringSimilarity_MLE function has 8 additional metrics: -OSA: OptimalStringAlignment -DL: Damerau-Levenshtein Distance -JACCARD: Jaccard Similarity -COSINE: Cosine Similarity -HAMMING: Hamming Distance -LDWS: Levenshtein Distance without Substitution -LCS: LongestCommonSubstring -SOUNDEXCODE: Soundex Code based Similarity (only for English strings).
ANLY-8244	**Description**: For KNN function, automatic tuning of PartitionBlockSize might not be optimal. **Workaround**: Manually tune value of PartitionBlockSize.
ANLY-6958	**Description**: If an error message exceeds 256 characters, it is truncated to 256 characters. **Workaround**: None.

Server Management

Reference ID	Description
SM-29354	Updating Spring Framework to resolve CVE-2020-5398 (BDSA-2020-0069) **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. **Deployments**: All
SM-28655	Update Apache log4j for CVE-2019-17571 (BDSA-2019-4008) **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. Apache workaround: https://nsfocusglobal.com/apache-log4j-deserialization-remote-code-execution-cve-2019-17571-vulnerability-threat-alert/ **Deployments**: All

Advanced SQL Engine Analytic Functions

Reference ID	Description
TDAF-287	**Description**: Function arguments that specify multiple columns accept only lists of column names, not column ranges or a combination of column names and column ranges. **Workaround**: None.

Advanced SQL Engine

Reference ID	Description
DBSQ-3762	**Description**: Error messages show old, nonstandardized argument and table names. **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 AppCenter

Reference ID	Description
UDAPP-8661	**Description**: Customer will need to delete the malformed prometheus data to resolve errors in thanos compactor **Workaround** - Remove the corrupted blocks and restart thanos compactor
UDAPP-8648	**Description**: Ambassador needs to be restarted once new certificates are installed. This issue is intermittent. **Workaround**: Restart ambassador pods, only If the the browser does not show updated certificates after install.
UDAPP-8601	**Description**: Apps with permissions revoked are visible to user, but if clicked it will throw permission error. **Workaround**: None.
UDAPP-8552	**Description**: Multibyte character app names do not work. **Workaround**: None.
UDAPP-8270	**Description**: Scheduled and Manual backups fail if Postgres data size is very large. If node does not have twice the space that Postgres has, backup fails with OOM or Pod Evicted. **Workaround**: Free up space in /var/lib/docker mount on machine where backup pods run. The space in this folder must be twice the size of the Postgres data.
UDAPP-8206	**Description**: Execution of OS commands is blocked from BTEQ apps. The . OS directive on BTEQ apps does not execute, but job shows status as successful. **Workaround**: Do not rely on job status when using BTEQ apps with . OS directive. Instead, see logs of apps, which display error messages related to failure in command execution.
UDAPP-8119	**Description**: Postgres fails to store large results. **Workaround**: Reduce size of query or split query into multiple parts.
UDAPP-7789	**Description**: Parsing fails for parameters with double hyphens. **Workaround**: None.
UDAPP-7192	**Description**: Service accounts in AppCenter are not backed up by Scheduled or Manual backup. **Workaround**: Manually recreate all service accounts in AppCenter after restore.

Vantage

Reference ID	Description
VAN-31	**Description**: If table being transferred from NewSQL Engine to ML Engine has VARBYTE column and type of corresponding ML Engine column is incompatible with VARBYTE, error message says Found: bytea instead of Found: varbyte ; for example: NAIVEBAYESPREDICT: The column 'c_varbyte' specified in CategoricalInputs must be a member of one of the following SQL type groups: [INTEGER, STRING]. Found: bytea **Workaround**: On ML Engine, change column type from VARBYTE to BYTEA by calling procedure TD_SYSFNLIB.QGExecuteForeignQuery .

Teradata Viewpoint

Reference ID	Description
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) **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." **Deployments**: All
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. **Workaround**: None. **Deployments**: All

VP-50514	**Description**: Upgrade to Tomcat 9.0.30 to address the following high (CVSS >=7.0) security risks: * CVE-2019-17563 (BDSA-2019-4037) **Workaround**: N/A Ease of exploitation: Very difficult. From the CVE, "The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability." While it is possible, it is unlikely. **Deployments**: All