Cloudera Flow Management 2.0.1

Cloudera Flow Management Release Notes

Date published: 2019-06-26
Date modified: 2021-01-06

https://docs.cloudera.com/

Legal Notice

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

What's New in This Release?

Cloudera Flow Management (CFM) 2.0.1 includes new Apache NiFi features and improvements.

CDP Data Center support

CFM 2.0.1 offers NiFi and NiFi Registry for deployment on CDP Private Cloud Base for the first time.

Apache NiFi Updates

Note: The NiFi version in CFM 2.0.1 is NiFi 1.11.4.2.0.1.0. It means that CFM 2.0.1 is based on Apache NiFi 1.11.4 but it also includes additional features, improvements, and fixes.

New features and improvements in Apache NiFi include:

- Parameters. The parameters are a new concept in NiFi that allows users to define Parameter Contexts attached to process groups so that any property (including sensitive properties and properties not supporting expression language) can be parameterized. This is particularly useful in CI/CD pipelines when deploying workflows across multiple environments. Parameters should be used as a replacement of the variables.
- Predictive monitoring. NiFi has now an internal analytics framework which can be enabled to predict back pressure occurrence, given the configured settings for threshold on a queue. It uses recent observations from a queue (either number of objects or content size over time) and calculates predictions based on a model to anticipate backpressure.

  For more details on analytics properties, see Analytics Properties.
- Rules engine (Technical Preview). It is now possible to define a Rules Engine controller service to support execution of a centralized set of rules (stored as files or provided within the service configuration) against a provided set of data called facts. Upon execution, the rules engine will determine what rules have been met and return a list of actions that should be executed based on the conditions defined within the rules. This is particularly useful for workflow monitoring.
- Content and FlowFile repositories encryption (Technical Preview). In addition to the Provenance repository it is now possible to encrypt both Content and FlowFile repositories on disks to comply with strict security requirements. This feature is in technical preview.

  For more details on FlowFile repository properties, see Encrypted Write Ahead FlowFile Repository Properties.

  For more details on content repository properties, see Encrypted File System Content Repository Properties.
- SQL reporting task. The QueryNiFiReportingTask allows users to execute SQL queries against tables containing information on Connection Status, Processor Status, Bulletins, Process Group Status, JVM Metrics, Provenance and Connection Status Predictions. In combination with Site to Site, it is particularly useful to define fine-grained monitoring capabilities on top of the running workflows.

Component support

List of the official component versions for Cloudera Flow Management. To know the component versions for compatibility with other applications, you must be familiar with the latest component versions in CFM.

CFM 2.0.1

- Apache NiFi 1.11.4
- Apache NiFi Registry 0.6.0

Note:

NiFi works with the version of NiFi Registry shipped with your version of CFM or later.

Unsupported Features

The following features are developed and tested by the Cloudera community but are not officially supported by Cloudera. These features are excluded for a variety of reasons, including insufficient reliability or incomplete test case coverage, declaration of non-production readiness by the community at large, and feature deviation from Cloudera best practices. Do not use these features in your production environments.

Technical Preview Features

The following features are available within CFM 2.0.1 but are not ready for production deployment. Cloudera encourages you to explore these technical preview features in non-production environments and provide feedback on your experiences through the Cloudera Community Forums.

- Knox integration with NiFi
- Encrypted flow file repository
- Encrypted content repository
- The following rules engine and handlers controller services:
    - EasyRulesEngineService
    - EasyRulesEngineProvider
    - ScriptedRulesEngine
    - ActionHandlerLookup
    - AlertHandler
    - ExpressionHandler
    - LogHandler
    - RecordSinkHandler
    - ScriptedActionHandler

Unsupported Customizations

Cloudera cannot guarantee that default NiFi processors are compatible with proprietary protocol implementations or proprietary interface extensions. For example, we support interfaces like JMS and JDBC that are built around standards, specifications, or open protocols. But we do not support customizations of those interfaces, or proprietary extensions built on top of those interfaces.

Apache Patches

The following sections list patches in each CFM component beyond what was fixed in the base version of the Apache component.

NiFi Patches

This release includes Apache NiFi 1.11.4 and the following patches.

- NIFI-4792: Allow QueryRecord processor to query nested arrays.
- NIFI-6064: MockComponentLog misplaces reported exceptions.
- NIFI-6491: Improve installation documentation.
- NIFI-6551: Improve timestamp handling for PutKudu processor.
- NIFI-6867: PutKudu operation type parameter allows bad values.

- NIFI-6927: PutElasticsearchHttp 1.10.0 with java 11 Fails to initialize due to "clientBuilder.sslSockerFactory(SSLSocketFactory) not supported on JDK 9+.
- NIFI-6958: Disabled State in Registry (in Sub PG) breaks Flow Update on Nifi Side.
- NIFI-6968: Create Connection Modal Allows Multiple Adds.
- NIFI-7049: SFTP processors shouldn't silently try to access known hosts file of the user.
- NIFI-7053: Update Toolkit Guide with macOS 10.15 trusted certificate requirements (2048 bit key and max of 825 days of validity).
- NIFI-7067: Allow a user and group with the same name/identity to exist.
- NIFI-7075: Update list of flowfile core attributes in Developer Guide.
- NIFI-7082: In tls-toolkit, change default validity of to 825 days or less.
- NIFI-7095: ResetSetRecordSet: handle java.sql.Array Types in normalizeValue method.
- NIFI-7105: NPE in SiteToSiteStatusReportingTask for counters.
- NIFI-7106: Add parent name and parent path in SiteToSiteStatusReportingTask.
- NIFI-7108: Upgrade com.puppycrawl.tools:checkstyle.
- NIFI-7109: Unit tests should be able to determine if item validator was called.
- NIFI-7114: NiFi not closing file handles.
- NIFI-7117: Load Balance is not working.
- NIFI-7132: PutCassandraQL is handling UUIDs as Strings.
- NIFI-7135: Fix Java 11 build with com.puppycrawl.tools:checkstyle:jar:8.29 dependency.
- NIFI-7136: Set the autocomplete HTML5 tag to false for username/password login fields.
- NIFI-7142: Automatically handle schema drift in the PutKudu processor.
- NIFI-7143: Upgrade GCP dependency.
- NIFI-7157: Investigate adoption of Github Workflow - Actions - CI.
- NIFI-7165: Update documentation for Toolkit certificate validity period to 825 days.
- NIFI-7175: Fix formatting of core attributes in docs.

For more information on fixed Apache NiFi patches, see the Apache NiFi Release Notes.

NiFi Registry Patches

This release includes Apache NiFi Registry 0.6.0 and the following patches.

- NIFIREG-252: Add docker maven image and build profile.
- NIFIREG-320: Add standard HTTP security headers.
- NIFIREG-323: Updated bootstrap port handling causes restarts to fail.
- NIFIREG-325: Support for node identity group.
- NIFIREG-334: Changes to support Java 11.
- NIFIREG-336: Enable Integration Tests by Default.
- NIFIREG-353: Add ShellUserGroupProvider to NiFi Registry.
- NIFIREG-355: Include profiles for hadoop libs in ranger plugin.
- NIFIREG-356: Fixing additional classpath resources for Authorizers.
- NIFIREG-358: Proxy authorization not working with groups.

For more information on fixed Apache NiFi Registry patches, see the Apache NiFi Registry Release Notes.

Known Issues

Summarizes known issues for this release.

JDK limitation

JDK 8u271, JDK 8u281, and JDK 8u291 may cause socket leak issues in NiFi due to JDK-8245417 and JDK-8256818. Pay attention to the build version of your JDK because some later builds are fixed as described in JDK-8256818.

Workaround: Consider using a more recent version of the JDK like 8u282, or builds of the JDK where the issue is fixed.

ReplaceText with multiple concurrency tasks can result in data corruption

ReplaceText, when scheduled to run with multiple Concurrent Tasks, and using a Replacement Strategy of "Regular Expression" or "Literal Replace" can result in content being corrupted.

The issue is far more likely to occur with multiple Concurrent Tasks, but it may be possible to trigger when using a single Concurrent Task.

To get the fix for this issue, file a support case through the Cloudera portal.

NiFi Registry start issue

When you upgrade CFM, NiFi Registry might fail during the start with the following error message:

```
Caused by: org.xml.sax.SAXParseException: cvc-complex-type.2.4.b
: The content of element 'providers' is not complete. One of '{e
ventHookProvider, extensionBundlePersistenceProvider}' is expect
ed.
```

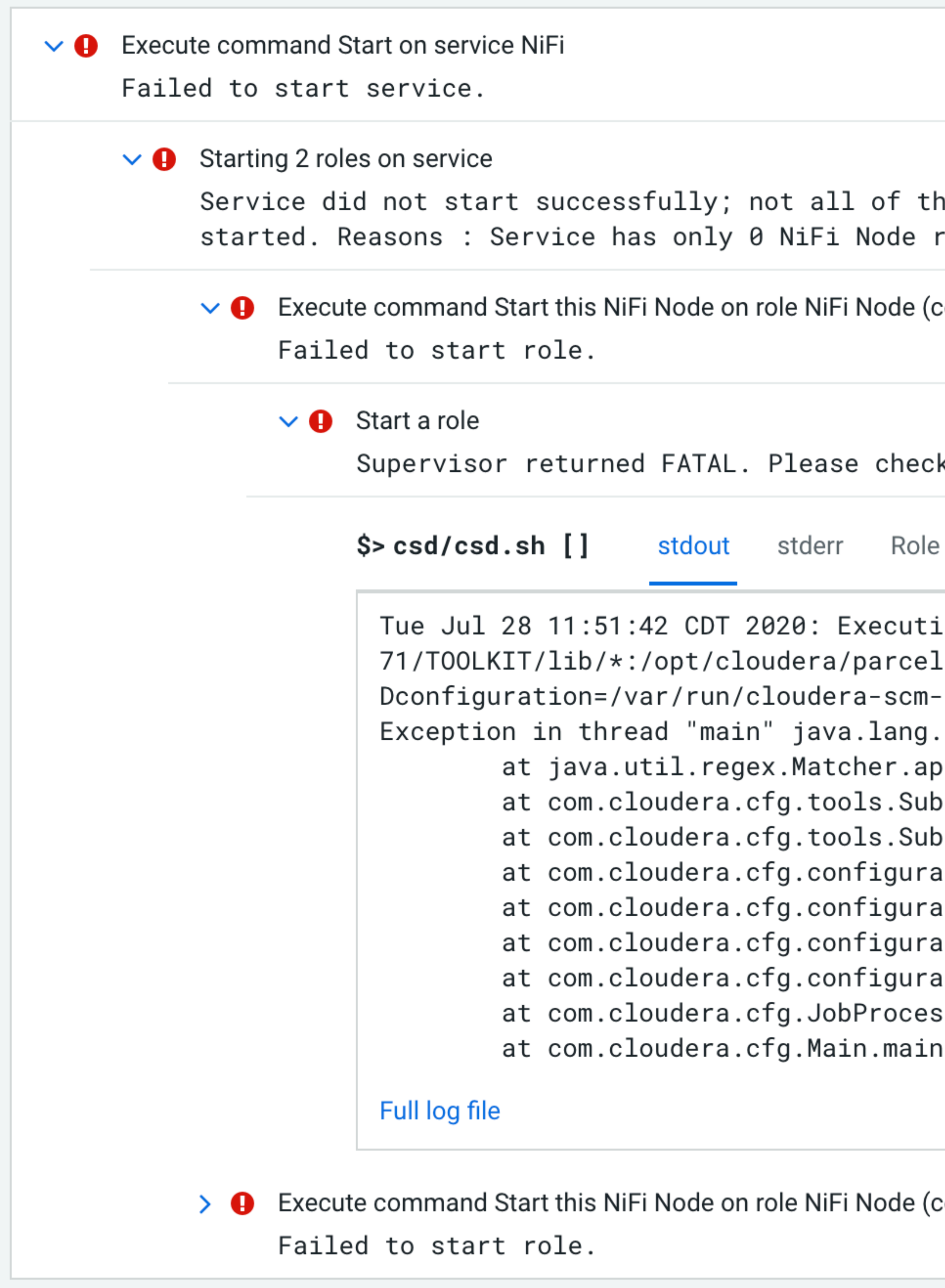
To resolve this issue:

1. Go to the NiFi Registry Advanced Configuration Snippet (Safety Valve) section in Cloudera Manager for staging/providers.xml.
2. Click View as XML and paste the following configuration in the template:

```
<property>
<name>xml.providers.extensionBundlePersistenceProvider.file-b
undle-provider.class</name>
<value>org.apache.nifi.registry.provider.extension.FileSyste
mBundlePersistenceProvider</value>
</property>
<property>
<name>xml.providers.extensionBundlePersistenceProvider.file-bu
ndle-provider.property.Extension Bundle Storage Directory</n
ame>
<value>${nifi.registry.working.directory}/extension_bundles</
value>
</property>
```

NiFi start issue

If the master key password or LDAP manager password contains a $ character, Cloudera Manager will fail to start NiFi. The following image shows the error messsage:



Execute command Start on service NiFi

Failed to start service.

Starting 2 roles on service

Service did not start successfully; not all of th
started. Reasons : Service has only 0 NiFi Node r

Execute command Start this NiFi Node on role NiFi Node (c

Failed to start role.

Start a role

Supervisor returned FATAL. Please check

```
Tue Jul 28 11:51:42 CDT 2020: Executi
71/TOOLKIT/lib/*:/opt/cloudera/parcel
Dconfiguration=/var/run/cloudera-scm-
Exception in thread "main" java.lang.
        at java.util.regex.Matcher.ap
        at com.cloudera.cfg.tools.Sub
        at com.cloudera.cfg.tools.Sub
        at com.cloudera.cfg.configura
        at com.cloudera.cfg.configura
        at com.cloudera.cfg.configura
        at com.cloudera.cfg.configura
        at com.cloudera.cfg.JobProces
        at com.cloudera.cfg.Main.main
```

Execute command Start this NiFi Node on role NiFi Node (c

Failed to start role.

To resolve, remove or replace the $ in the password.

Base cluster and compute cluster names must not have white space

When you create your base cluster or compute cluster, ensure that the cluster name does not contain any white space.

Ranger audits for NiFi and NiFi Registry

After you install NiFi and NiFi Registry, complete the following steps to ensure that Ranger audits are stored correctly in HDFS:

NiFi:

1. Go to the NiFi Actions menu and trigger the Create Ranger NiFi Plugin Audit Directory service command.
2. Go to the NiFi Configuration page and set "xml.authorizers.authorizer.ranger-provider.classpath" = "${CONF_DIR}/hadoop-conf".
3. Restart NiFi.

NiFi Registry:

1. NiFi Registry must be installed with a NiFi dependency. Only in this case, the NiFi Registry config directory will contain the hadoop-conf directory with related HDFS configurations. Check that this directory is available.
2. Connect to the host with NiFi Registry and run the following HDFS commands:

```
hadoop fs -mkdir /ranger/audit/nifi-registry
hadoop fs -chown nifiregistry:nifiregistry /ranger/audit/nifi-
registry
hadoop fs -chmod 755 /ranger/audit/nifi-registry
```

3. Go to Cloudera Manager UI on the NiFi Registry Configiuration page and set "xml.authorizers.authorizer.ranger-provider.classpath" = "${CONF_DIR}/hadoop-conf".
4. Restart NiFi Registry.

Ranger High Availability

If you have multiple instances of the Ranger Admin service and if the ranger_rest_url parameter contains a comma separated list of URLs (i.e. the Ranger instances are not behind a load balancer), then NiFi and NiFi Registry will not start and the following error appears in Cloudera Manager:

```
Traceback (most recent call last):
File "/var/run/cloudera-scm-agent/process/1546471613-nifiregistry
-NIFI_REGISTRY_SERVER/scripts/ranger.py", line 683, in <module>
main()
File "/var/run/cloudera-scm-agent/process/1546471613-nifiregistry
-NIFI_REGISTRY_SERVER/scripts/ranger.py", line 633, in main
keytab=args.keytab, principal=args.principal)
File "/var/run/cloudera-scm-agent/process/1546471613-nifiregis
try-NIFI_REGISTRY_SERVER/scripts/ranger.py", line 302, in create
_ranger_repository
_create()
File "/var/run/cloudera-scm-agent/process/1546471613-nifiregist
ry-NIFI_REGISTRY_SERVER/scripts/ranger.py", line 291, in _create
ranger_service_name, code, out))
Exception: Failed to create ranger repository 'Lower Environme
nt_nifiregistry', response code is '404', output is ''.
```

To resolve, place the Ranger instances behind a load balancer. Alternatively, create a support case on the Cloudera Support portal.

Technical Service Bulletins

TSB 2022-580: NiFi Processors cannot write to content repository

If the content repository disk is filled more than 50% (or any other value that is set in nifi.propert ies for nifi.content.repository.archive.max.usage.percentage), and if there is no data in the content repository archive, the following warning message can be found in the logs: "Unable to write flowfile content to content repository container default due to archive file size constraints; waiting for archive cleanup". This would block the processors and no more data is processed.

This appears to only happen if there is already data in the content repository on startup that needs to be archived, or if the following message is logged: “Found unknown file XYZ in the File System Repository; archiving file”.

Upstream JIRA

- NIFI-10023
- NIFI-9993

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: TSB 2022-580: NiFi Processors cannot write to content repository

TSB 2022-589: CVE-2022-33140 Apache NiFi ShellUserGroupProvider Vulnerability

The optional ShellUserGroupProvider in Apache NiFi 1.10.0 to 1.16.2 and Apache NiFi Registry 0.6.0 to 1.16.2 does not neutralize arguments for group resolution commands, allowing injection of operating system commands on Linux and macOS platforms. The ShellUserGroupProvider is not included in the default configuration. Command injection requires ShellUserGroupProvider to be one of the enabled User Group Providers (UGP) in the Authorizers configuration. Command injection also requires an authenticated user with elevated privileges. Apache NiFi requires an authenticated user with authorization to modify access policies in order to execute the command. Apache NiFi Registry requires an authenticated user with authorization to read user groups in order to execute the command. The resolution removes command formatting based on user-provided arguments.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: TSB 2022-589: CVE-2022-33140 Apache NiFi ShellUserGroupProvider Vulnerability

Related Information

Cloudera Support

Fixed Issues

Because this is the first release in CFM 2.0.x release line, there are no fixed issues.

Common Vulnerabilities and Exposures

Lists common vulnerabilities and exposures fixed in CFM 2.0.1.

CVE-2020-9486

Component: Apache NiFi

Description: The NiFi stateless execution engine produced log output which included sensitive property values. When a flow was triggered, the flow definition configuration JSON was printed, potentially containing sensitive values in plaintext.

Severity: Important

Versions Affected: Apache NiFi 1.10.0 - 1.11.4

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-9486

CVE-2020-9487

Component: Apache NiFi

Description: The NiFi download token (one-time password) mechanism used a fixed cache size and did not authenticate a request to create a download token, only when attempting to use the token to access the content. An unauthenticated user could repeatedly request download tokens, preventing legitimate users from requesting download tokens.

Severity: Important

Versions Affected: Apache NiFi 1.10.0 - 1.11.4

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-9487

CVE-2020-9491

Component: Apache NiFi

Description: The NiFi UI and API were protected by mandating TLS v1.2, as well as listening connections established by processors like ListenHTTP, HandleHttpRequest, etc. However intracluster communication such as cluster request replication, Site-to-Site, and load balanced queues continued to support TLS v1.0 or v1.1.

Severity: Critical

Versions Affected: Apache NiFi 1.2.0 - 1.11.4

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-9491

CVE-2020-11023

Component: Apache NiFi

Description: The jquery dependency had an XSS vulnerability. See NIST NVD CVE-2020-11023 for more information.

Severity: Low

Versions Affected: Apache NiFi 1.8.0 - 1.11.4

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-11023

CVE-2019-9658

Component: Apache NiFi

Description: The com.puppycrawl.tools:checkstyle dependency had a XXE vulnerability. See NIST NVD CVE-2019-9658 for more information.

Severity: Low

Versions Affected: Apache NiFi 1.8.0 - 1.11.4

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-9658

CVE-2019-11358

Component: Apache NiFi

Description: Various vulnerabilities existed within the JQuery dependency used by NiFi. See NIST NVD CVE-2019-11358 for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.6.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-11358

CVE-2019-10247, CVE-2019-10246

Component: Apache NiFi

Description: Various vulnerabilities existed within the Jetty dependency used by NiFi. See NIST NVD CVE-2019-10247, NIST NVD CVE-2019-10246 for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.8.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-10247

CVE-2019-16335, CVE-2019-14540, CVE-2019-14439, CVE-2019-12814, CVE-2019-12384, CVE-2018-1000873, CVE-2018-19362, CVE-2018-19361, CVE-2018-19360

Component: Apache NiFi

Description: Various vulnerabilities existed within the Jackson Core: Databind dependency used by NiFi. See NIST NVD CVE-2019-16335, NIST NVD CVE-2019-14540, NIST NVD CVE-2019-14439, NIST NVD CVE-2019-12814, NIST NVD CVE-2019-12384, NIST NVD CVE-2018-1000873, NIST NVD CVE-2018-19362, NIST NVD CVE-2018-19361, NIST NVD CVE-2018-19360 for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-16335

CVE-2019-0193, CVE-2019-0192, CVE-2017-3164

Component: Apache NiFi

Description: Various vulnerabilities existed within the Solr dependency used by NiFi. See NIST NVD CVE-2019-0193, NIST NVD CVE-2019-0192, NIST NVD CVE-2017-3164 for more information.

Severity: Critical

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-0193

CVE-2017-5637, CVE-2016-5017, CVE-2018-8012

Component: Apache NiFi

Description: Various vulnerabilities existed within the Zookeeper dependency used by NiFi. See NIST NVD CVE-2018-8012, NIST NVD CVE-2017-5637, NIST NVD CVE-2016-5017 for more information.

Severity: Important

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2017-5637

CVE-2019-10083

Component: Apache NiFi

Description: When updating a Process Group via the API, the response to the request includes all of its contents (at the top most level, not recursively). The response included details about processors and controller services which the user may not have had read access to.

Severity: Low

Versions Affected: Apache NiFi 1.3.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-10083

CVE-2019-12421

Component: Apache NiFi

Description: If NiFi uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi.

Severity: Moderate

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-12421

CVE-2019-10080

Component: Apache NiFi

Description: The XMLFileLookupService allowed trusted users to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE) and reveal information such as the versions of Java, Jersey, and Apache that the NiFI instance uses.

Severity: Low

Versions Affected: Apache NiFi 1.3.0 - 1.9.2

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-10080

CVE-2019-10768

Component: Apache NiFi

Description: An Object.prototype pollution vulnerability existed within the AngularJS dependency used by NiFi. See NIST NVD CVE-2019-10768 for more information.

Severity: Important

Versions Affected: Apache NiFi 1.8.0 - 1.10.0

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2019-10768

CVE-2020-1933

Component: Apache NiFi

Description: Malicious scripts could be injected to the UI through action by an unaware authenticated user in Firefox. Did not appear to occur in other browsers.

Severity: Important

Versions Affected: Apache NiFi 1.0.0 - 1.10.0

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-1933

CVE-2020-1928

Component: Apache NiFi

Description: The sensitive parameter parser would log parsed property descriptor values for debugging purposes. This would expose literal values entered in a sensitive property when no parameter was present.

Severity: Moderate

Versions Affected: Apache NiFi 1.10.0

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-1928

CVE-2020-1942

Component: Apache NiFi

Description: The flow fingerprint factory generated flow fingerprints which included sensitive property descriptor values. In the event a node attempted to join a cluster and the cluster flow was not inheritable, the flow fingerprint of both the cluster and local flow was printed, potentially containing sensitive values in plaintext.

Severity: Important

Versions Affected: Apache NiFi 0.0.1 - 1.11.0

Apache CVE Report Link: https://nifi.apache.org/security.html#CVE-2020-1942

Download from the CFM Repository

Use the following tables to identify the Cloudera Flow Management (CFM) repository location for your operating system and operational objectives.

Note:

You must have the credentials to download the files. Your download credentials are not the same as the credentials you use for the support portal.

You can get the credentials in the following ways:

- Contact your Cloudera sales representative.
- View the Welcome email for your Flow Management account.
- File a non-technical case within the Cloudera support portal for our Support team to assist you.

Table 1: CentOS 7

File	Location
Manifest	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/parcel/manifest.json
Parcel	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/parcel/CFM-2.0.1.0-71-el7.parcel
Sha File	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/parcel/CFM-2.0.1.0-71-el7.parcel.sha

Table 2: CSD Files

File	Location
NiFi CSD File	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/parcel/NIFI-1.11.4.2.0.1.0-71.jar
NiFi Registry CSD File	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/parcel/NIFIREGISTRY-0.6.0.2.0.1.0-71.jar

Table 3: Standalone components

File	Location
NiFi (.tar.gz)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-1.11.4.2.0.1.0-71-bin.tar.gz
NiFi (.zip)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-1.11.4.2.0.1.0-71-bin.zip
NiFi (.zip SHA256)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-1.11.4.2.0.1.0-71-bin.zip.sha256

File	Location
NiFi Registry (.tar.gz)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi_registry/nifi-registry-0.6.0.2.0.1.0-71-bin.tar.gz
NiFi Toolkit (.tar.gz)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-toolkit-1.11.4.2.0.1.0-71-bin.tar.gz
NiFi Toolkit (.zip)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-toolkit-1.11.4.2.0.1.0-71-bin.zip
NiFi Toolkit (zip SHA256)	https://archive.cloudera.com/p/CFM/centos7/2.x/updates/2.0.1.0/tars/nifi/nifi-toolkit-1.11.4.2.0.1.0-71-bin.zip.sha256

Table 4: Windows Files

File	Location
NiFi (.msi)	https://archive.cloudera.com/p/CFM/2.0.1.0/nifi-2.0.1.0-71.msi