B2B Solutions
Let's build IT together

Integration News

T1 2024

In this issue:

IBM Sterling B2B Data Exchange Solutions. SECURITY NEWS:

IBM Sterling Connect:Direct for UNIX is vulnerable to unspecified vulnerabilities and sensitive information exposure due to IBM Runtime Environment Java Technology Edition Version 17.

CVEID: CVE-2024-20932
CVEID: CVE-2024-20952
CVEID: CVE-2024-20918
CVEID: CVE-2024-20921
CVEID: CVE-2024-20926
CVEID: CVE-2024-20945
CVEID: CVE-2024-22361

IBM Sterling B2B Integrator dashboard is vulnerable to cross-site request forgery.

CVEID: CVE-2019-11358

IBM Sterling B2B Integrator is affected by vulnerability in JDOM

CVEID: CVE-2021-33813

IBM Sterling B2B Integrator affected by XStream security vulnerabilities.

CVEID: CVE-2022-41966
CVEID: CVE-2022-40151
CVEID: CVE-2022-40152
CVEID: CVE-2022-40153
CVEID: CVE-2022-40154
CVEID: CVE-2022-40155
CVEID: CVE-2022-40156

IBM Sterling B2B Integrator affected by FasterXML Jackson-data vulnerabilities

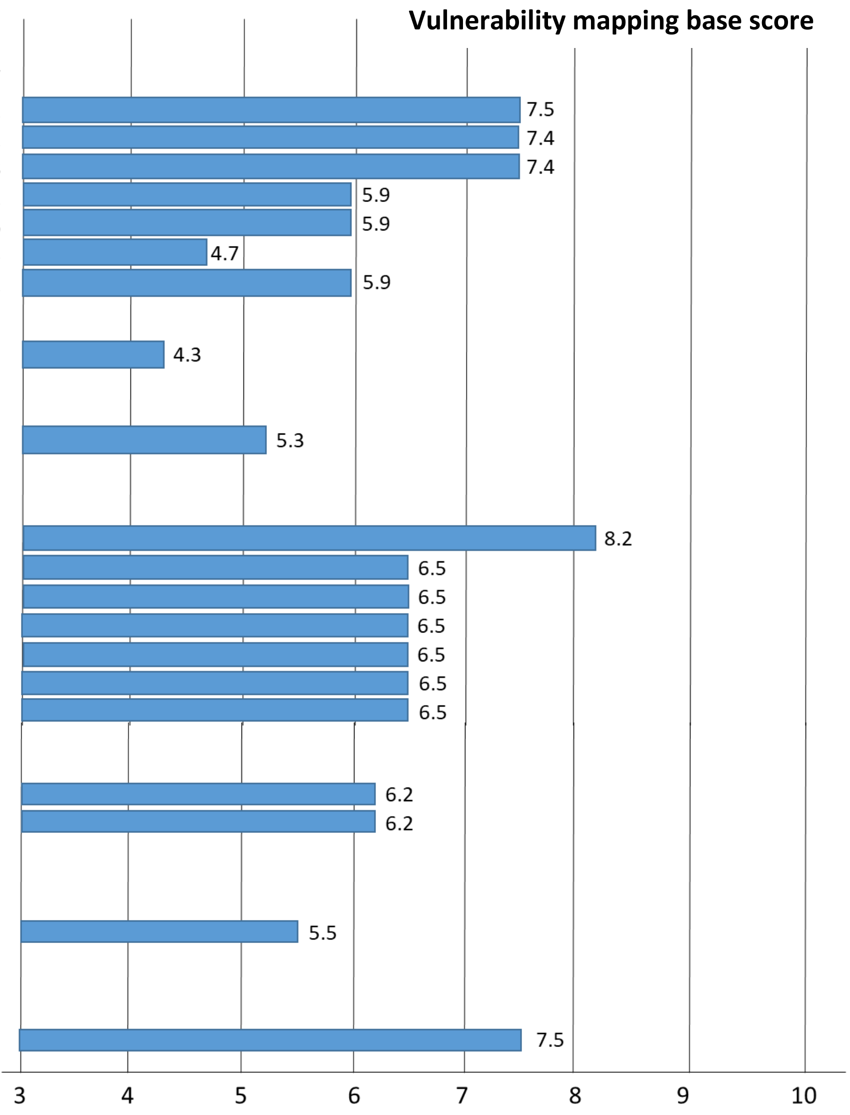
CVEID: CVE-2022-42004
CVEID: CVE-2024-42003

IBM Sterling B2B Integrator is affected by sensitive information exposure due to Apache James MIME4J

CVEID: CVE-2019-11358

IBM Sterling B2B Integrator is vulnerable to denial of service due to Apache Commons FileUpload

CVEID: CVE-2019-11358



Other contents:

- What's new in IBM Sterling B2B Integrator 6.2.0.1
- Fix List for Sterling B2B Integrator V6.2.0.0
- Troubleshooting. IBM Sterling B2B Integrator. How to manually stop and start the Liberty server used in Rest API?
- IBM B2B Integrator / IBM Sterling File Gateway. Releases dates.
- Troubleshooting. IBM Sterling Control Center Monitor.Control Center reporting Connect:Direct Server is down.

IBM Sterling Connect:Direct for UNIX is vulnerable to unspecified vulnerabilities and sensitive information exposure due to IBM Runtime Environment Java Technology Edition Version 17

IBM Java 17 is used by IBM Sterling Connect:Direct for UNIX in product configuration and management. IBM Sterling Connect:Direct for UNIX is impacted by unspecified vulnerabilities and sensitive information exposure due to IBM Java 17. IBM Sterling Connect:Direct for UNIX has upgraded IBM Java 17 to address the issues.

Vulnerability Details

CVEID: CVE-2024-20932

Description: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause high integrity impact.

CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2024-20952

Description: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause high confidentiality impact and high integrity impact.

CVSS Base score: 7.4
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2024-20918

Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact and high integrity impact.

CVSS Base score: 7.4
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2024-20921

Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact.

CVSS Base score: 5.9
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2024-20926

Description: An unspecified vulnerability in Java SE related to the Scripting component could allow a remote attacker to cause high confidentiality impact.

CVSS Base score: 5.9
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2024-20945

Description: An unspecified vulnerability in Java SE related to the VM component could allow a local authenticated attacker to cause high confidentiality impact.

CVSS Base score: 4.7
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2024-22361

Description: IBM Semeru Runtime 8.0.302.0 through 8.0.392.0, 11.0.12.0 through 11.0.21.0, 17.0.1.0 - 17.0.9.0, and 21.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 281222.

CVSS Base score: 5.9
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.0.0.0 - 6.0.0.2.iFix163
	6.1.0.0 - 6.1.0.4.iFix104

Remediation/Fixes

IBM strongly recommends addressing the vulnerability now by upgrading

Version	Remediation/Fix/ Instructions
6.1.0.0 - 6.1.0.4.iFix104	Apply 6.1.0.4.iFix106, available here.
6.0.0.0 - 6.0.0.2.iFix163	Apply 6.1.0.4.iFix106, available here.

Workarounds and Mitigations
None.

IBM Sterling B2B Integrator dashboard is vulnerable to cross-site request forgery

IBM Sterling B2B Integrator has addressed the cross-site request forgery security vulnerability within dashboard.

Vulnerability Details

CVEID: CVE-2022-35638

Description: IBM Sterling B2B Integrator Standard Edition is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.

CVSS Base score: 4.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.8
	6.1.0.0 - 6.1.2.1

Remediation/Fixes

Version	Remediation & Fix
6.0.0.0 - 6.0.3.8	Apply 6.0.3.9
6.1.0.0 - 6.1.2.1	Apply 6.1.2.3 or 6.2.0.0

The IIM versions of 6.0.3.9 and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage.

The container version of 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations
None.

IBM Sterling B2B Integrator is affected by vulnerability in JDOM

IBM Sterling B2B Integrator uses JDOM.

Vulnerability Details

CVEID: CVE-2021-33813

Description: JDOM is vulnerable to a denial of service, caused by an XXE issue in SAXBuilder. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to cause the a denial of service.

CVSS Base score: 5.3
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.8
	6.1.0.0 - 6.1.0.6, 6.1.1.0 - 6.1.1.1 and 6.1.2.0

Remediation/Fixes

Version	Remediation & Fix
6.0.0.0 - 6.0.3.8	Apply 6.0.3.9
6.1.0.0 - 6.1.0.6, 6.1.1.0 - 6.1.1.1 and 6.1.2.0	Apply 6.1.0.8, 6.1.1.4, 6.1.2.3 or 6.2.0.0

The IIM versions of 6.0.3.9, 6.1.0.8, 6.1.1.4, and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage

The container version of 6.1.0.8, 6.1.1.4, 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations
None.

IBM Sterling B2B Integrator affected by XStream security vulnerabilities

IBM Sterling B2B Integrator uses XStream.

Vulnerability Details

CVEID: CVE-2022-41966

Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By manipulating the processed input stream at unmarshalling time, a remote attacker could exploit this vulnerability to replace or inject objects and cause a denial of service.

CVSS Base score: 8.2
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H))

CVEID: CVE-2022-40151

Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40152

Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40153

Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40154
Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40155
Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-40156
Description: XStream is vulnerable to a denial of service, caused by a stack-based buffer overflow. By sending a specially-crafted XML data, a remote authenticated attacker could exploit this vulnerability to causes the parser to crash, and results in a denial of service condition.

CVSS Base score: 6.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.8
	6.1.0.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.2

Remediation/Fixes

Version	Remediation/Fix/ Instructions
6.0.0.0 - 6.0.3.8	Apply 6.0.3.9
6.1.0.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.2	Apply 6.1.1.4, 6.1.2.3 or 6.2.0.0

The IIM versions of 6.0.3.9, 6.1.1.4, and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage.

The container version of 6.1.1.4, 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations

None.

IBM Sterling B2B Integrator affected by FasterXML Jackson-data vulnerabilities

IBM Sterling B2B Integrator uses FasterXML Jackson-databind.

Vulnerability Details

CVEID: CVE-2022-42004

Description: FasterXML jackson-databind is vulnerable to a denial of service, caused by a lack of a check in the BeanDeserializer._deserializeFromArray function. By sending a specially-crafted request using deeply nested arrays, a local attacker could exploit this vulnerability to exhaust all available resources.

CVSS Base score: 6.2
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2022-42003
Description: FasterXML jackson-databind is vulnerable to a denial of service, caused by a lack of a check in the primitive value deserializers when the UNWRAP_SINGLE_VALUE_ARRAYS feature is enabled. By sending a specially-crafted request using deep wrapper array nesting, a local attacker could exploit this vulnerability to exhaust all available resources.

CVSS Base score: 6.2
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.7
	6.1.0.0 - 6.1.0.6, 6.1.1.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.1

Remediation/Fixes

Version	Remediation/Fix/ Instructions
6.0.0.0 - 6.0.3.7	Apply 6.0.3.9

Version	Remediation/Fix/ Instructions
6.1.0.0 - 6.1.0.6, 6.1.1.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.1	Apply 6.1.0.8, 6.1.1.4, 6.1.2.3 or 6.2.0.0

The IIM versions of 6.0.3.9, 6.1.0.8, 6.1.1.4, and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage.

The container version of 6.1.1.4, 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations
None.

IBM Sterling B2B Integrator is affected by sensitive information exposure due to Apache James MIME4J

IBM Sterling B2B Integrator uses Apache James MIME4J.

Vulnerability Details

CVEID: CVE-2022-45787

Description: Apache James MIME4J could allow a local authenticated attacker to obtain sensitive information, caused by improper laxist permissions on the temporary files. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVSS Base score: 5.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.8
	6.1.0.0 - 6.1.0.7, 6.1.1.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.2

Remediation/Fixes

Version	APAR
6.0.0.0 - 6.0.3.8	IT43555
6.1.0.0 - 6.1.0.7, 6.1.1.0 - 6.1.1.3 and 6.1.2.0 - 6.1.2.2	

The IIM versions of 6.0.3.9, 6.1.0.8, 6.1.1.4, and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage.

The container version of 6.1.1.4, 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations
None.

IBM Sterling B2B Integrator is vulnerable to denial of service due to Apache Commons FileUpload

IBM Sterling B2B Integrator uses Apache Commons FileUpload.

Vulnerability Details

CVEID: CVE-2023-24998

Description: Apache Commons FileUpload and Tomcat are vulnerable to a denial of service, caused by not limit the number of request parts to be processed in the file upload function. By sending a specially-crafted request with series of uploads, a remote attacker could exploit this vulnerability to cause a denial of service condition.

CVSS Base score: 7.5
CVSS Temporal Score: Click here.
CVSS Vector:
(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	6.0.0.0 - 6.0.3.8
	6.1.0.0 - 6.1.0.7, 6.1.1.0 - 6.1.1.4 and 6.1.2.0 - 6.1.2.2

Remediation/Fixes

Version	APAR
6.0.0.0 - 6.0.3.8	IT43908
6.1.0.0 - 6.1.0.7, 6.1.1.0 - 6.1.1.4 and 6.1.2.0 - 6.1.2.2	

The IIM versions of 6.0.3.9, 6.1.0.8 and 6.1.2.3 are available on Fix Central. The IIM version of 6.2.0.0 is available on Passport Advantage.

The container version of 6.1.2.3 and 6.2.0.0 are available in IBM Entitled Registry.

Workarounds and Mitigations
None.

What's new in IBM Sterling B2B Integrator 6.2.0.1

This topic provides the new features and enhancements that are introduced in this release.

New features

Following new features are introduced in this release:

- Support for Adapters and Services to send and receive documents from Microsoft SharePoint.
- TLS v1.3 can now be configured for:
  - AS2 protocols.
  - B2B Mail Client Adapter.
  - EBICS Server.
  - EBICS Client.
  - FTP Server Adapter.
  - FTP Client Begin Session Service.
  - HTTPS Server Adapter.
  - HTTP Client Begin Session Service.
  - Microsoft SQL Server during the upgrade of Sterling B2B Integrator from v6.2.0.0 to v6.2.0.1 and above.
  - SSL-RMI. The default communication protocol is now configured as TLS 1.3 for Sterling B2B Integrator v6.2.0.1 and above.
  - Sterling B2B Integrator Dashboard logins.

> **Note:**
> - Future releases will include more adapters and services that support TLS 1.3.
> - The FIPS 140-2 standard does not define support for TLSv1.3 or the new cipher suites defined for it. Enabling both the TLSv1.3 protocol and FIPS support results in an error.

Java Development Kit (JDK) version is now upgraded to IBM JDK 8.0.8.15. This version should be used to install or upgrade to Sterling B2B Integrator v6.2.0.1. To download the IBM JDK for v6.2.0.1, use the SDK.zip file bundled along with the Media.

- Support for SSH keys using ssh-ed25519 key type for SFTP 2.0.
- Supports configuring B2B REST APIs to fetch more than 1000 records in the list API responses using the property maxRecordsLimit.
- Certified Container enhancements:
  - The minimum hardware requirements for installing Sterling B2B Integrator on Certified Container is now available.
  - Configure a specific SSL version using the property setupCfg.PROPERTY_security_SSLHelloProtocolin values.yaml.
  - Enable SSL logs using the properties asi.env.jvmOptions and setupCfg.PROPERTY_security_EnableSSLTrace in values.yaml.
  - Supports Autoscaling for Document Service.
  - Improved support for Command Line Adapter 2 (CLA2).

Stack updates

> **Note:**
> This mod pack also includes security fixes and stack upgrades from release 6125.

New security fixes and following stack upgrades are introduced in this release:

- Apache Axis - 2
- Apache POI - 5.2.3
- Apache Santuario (Java) - 2.3.4
- Apache Xerces - 2.12.2
- Bouncy Castle - 1.76
- IBM Installation Manager 1.9.2.6
- Java SDK/JRE - 8.0.8.15
- Jetty jars - 9.4.53
- JSON-java - 20231013
- Maverick Legacy Client and Server - 1.7.56
- MQ - 9.2.0.21
- Red Hat OpenShift Container Platform
  - Version 4.13.0 or later fixes
  - Version 4.14.0 or later fixes
- Kubernetes >= 1.26 and <= 1.28
- Helm - 3.13.x or later
- Spring Boot - 2.7.18
- Spring Framework - 5.3.31
- Spring Security jars - 5.8.9
- Struts - 2.5.33
- Velocity - 2.3

Fix List for Sterling B2B Integrator V6.2.0.0

This page contains comprehensive fix information for all Fix Packs released for Sterling B2B Integrator and Sterling File Gateway V6.2.0.0 and later versions.

Content
IBM periodically releases fix packs for download to resolve issues in Sterling B2B Integrator. All Sterling B2B Integrator customers should download the most recently available fix pack and apply it to their environments.

Follow these steps to update your system:

- Download the fix pack from Fix Central.
- Install the fix pack on each node in your environment. Remember that a node outage is required. You should apply the fix pack to your test environment first and run regression tests against it before applying it to production.
  - — Mod Pack (V6.2.0.0)
  - — Fix Pack (V6.2.0.1)

Mod Pack (v6.2.0.0)

Link	Date Released	Status
Download	September 22, 2023	Available

Note: This Mod Pack also contains APAR security and regular fixes from the release 6123.

Security Fixes

APAR	Description
IT43908	[ALL] APACHE COMMONS FILEUPLOAD (PUBLICLY DISCLOSED VULNERABILITY) (CVE-2023-24998 CVS 7.5)
IT43948	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44060	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44222	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44109	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44223	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43928	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT42896	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43937	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43649	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44156	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44139	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44182	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43976	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43916	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43990	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43591	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT40443	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43948	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44060	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44222	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44109	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44223	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43928	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT42896	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43937	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43649	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44156	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44139	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44182	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43976	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43916	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43990	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43591	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT40443	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44032	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT39127	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44185	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44139	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44297	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43950	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44078	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43522	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43549	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43138	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44079	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43972	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

APAR	Description
IT43941	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44081	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44091	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44441	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

Regular Fixes

APAR	Description
IT43785	NOT ABLE TO SEND EMAIL FROM STERLING INTEGRATOR / SBI / B2BI TO MS EXCHANGE ONLINE USING SMTP SEND ADAPTER
IT39345	OBSERVED SLOWNESS IN AS2 WITH LARGE FILE
IT42218	CREATE A ROUTING CHANNEL FOR A GLOBAL MAILBOX PARTNER VIA THE ROUTING CHANNEL REST API WHEN A DC IS DOWN
IT43645	GM IMPORT UTILITY FAILS WITH JAVA.LANG.NOCLASSDEFFOUNDERROR: ORG.APACHE.COMMONS.COLLECTIONS.ARRAYSTACK
IT43985	LOCAL_QUORUM ERROR AND FILE TRANSFERS ARE FAILING

Fix Pack (v6.2.0.1)

Link	Date Released	Status
Download	April 05, 2024	Available

Note: This Fix Pack also contains APAR security and regular fixes from the release 6125.

Security Fixes

APAR	Description
IT42806	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44862	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45244	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45233	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44889	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45045	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44144	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44671	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44198	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44322	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44559	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44899	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45197	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45204	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44415	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45242	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44282	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44789	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44310	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44092	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44315	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43508	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44317	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44312	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44304	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44311	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44283	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43138	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

APAR	Description
IT44284	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44287	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45496	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45500	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45519	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44078	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45521	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45449	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44182	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45491	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45485	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45619	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45620	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45621	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45450	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45690	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45673	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45722	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44733	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45059	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45979	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

Regular Fixes

APAR	Description
IT45184	CUSTOMATION PROPERTYUI ERROR - "INVALID VALUE SPECIFIED FOR FILE NAME !"
IT45145	STERLING B2B INTEGRATOR 6.2 MAP TEST THROWING ERROR - JAVAX.XML.SOAP.SOAPEXCEPTION
IT45178	FAILURES DURING SFTP PUT SERVICE ARE NOT SHOWN ON THE COMMUNICATION SESSION DETAILS SCREEN
IT44023	EBICS SERVER COF ORDERS ARE NOT VEU ENABLED
IT44045	EBICS SERVER - HPB FAILING FOR CLIENT IN PROD BECAUSE OF FILE FORMAT
IT44452	NO SECURITY RESPONSE HEADER FOUND IN THE HTTP RESPONSE FROM AN ADAPTER
IT45461	EDIINTPARSE BP FAILS WITH FAILURE UNPACKAGING MESSAGE ERROR - CLASS: 0; SUBCLASS: 0; CODE: 0;
IT45468	LINK ON THE MAIN B2BI DASHBOARD DIRECTS USERS TO 'QUESTIONABLE' SITE
IT45462	SSHKEYGRABBER - JAVA.LANG.NULLPOINTEREXCEPTION USING REMOTE PS ON 6.1.2.3
IT45670	ON UPGRADED INSTANCE FROM 6125 TO 6201, JDOM OLD VERSION JAR IS PRESENT
IT45444	GLOBAL MAILBOX MESSAGES NOT DELETED FROM PRODUCER MAILBOX WHEN ROUTED
IT45700	ITX LOGGING CAUSING SEVERE PERFORMANCE ISSUE
IT45730	CUSTOM JAR AND CUSTOM SERVICES JARS ARE FAILING TO INSTALL WHEN USING CUSTOMIZATION UI
IT45837	FAILURE TO CREATE DUMMY IFIX FOR B2BI 6201

Troubleshooting

IBM Sterling B2B Integrator
How to manually stop and start the Liberty server used in Rest API?

Steps

The rest API libery server running with B2Bi is stopped and restarted if you stop and restart B2Bi itself. If there is a need to restart the liberty server on its own, here is how you can perform that task:

— **Windows**

For Windows systems, you can simply stop and start the the service "IBM Sterling B2B Integrator Liberty Profile at nnnn" where nnnn is the port number where the Liberty server is running. Please wait for a moment after you stop the liberty server service to make sure that everything is stopped correctly before you start it again.

— **Linux**

1- Use the following command to stop the Liberty server:

```
<SterlingIntegrator_install_directory>/liberty/wlp/bin/server stop SIServer
```

Note: Make sure that you have set the JAVA_HOME system variable and that it points to the JAVA directory of the B2Bi installation: <SterlingIntegrator_install_directory>jdk

If you do not want to set this variable, you can kill the process manually, see below.

2- Check if any pid is still running and kill it if necessary with the command "kill -9 nnnn"

where nnnn is the pid of the liberty server.

3- Start the liberty server by using the startLiberty.sh script.

Note: when using the startLibery.sh script, if a pid is still running, the script will tell you what is the pid number still running so that you can kill it manually.

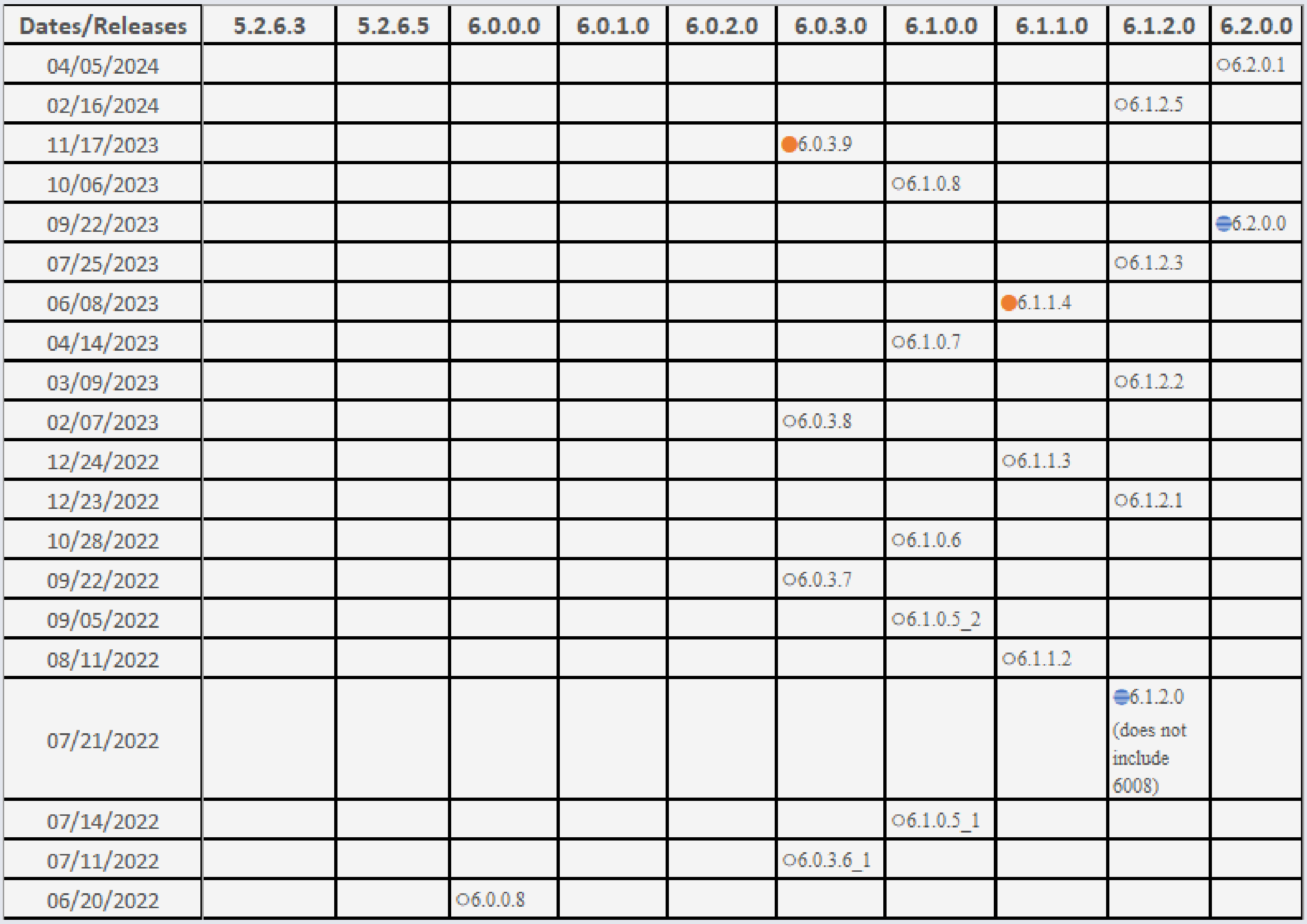
Alternatively, you can find the pid number information by checking the liberty server console log that can be found under: <SterlingIntegrator_install_directory>/liberty/wlp/usr/servers/SIServer/logs

Or by looking at the contents of the file SIServer.pid that can be found under: <SterlingIntegrator_install_directory>/liberty/wlp/usr/servers/.pid/SIServer.pid

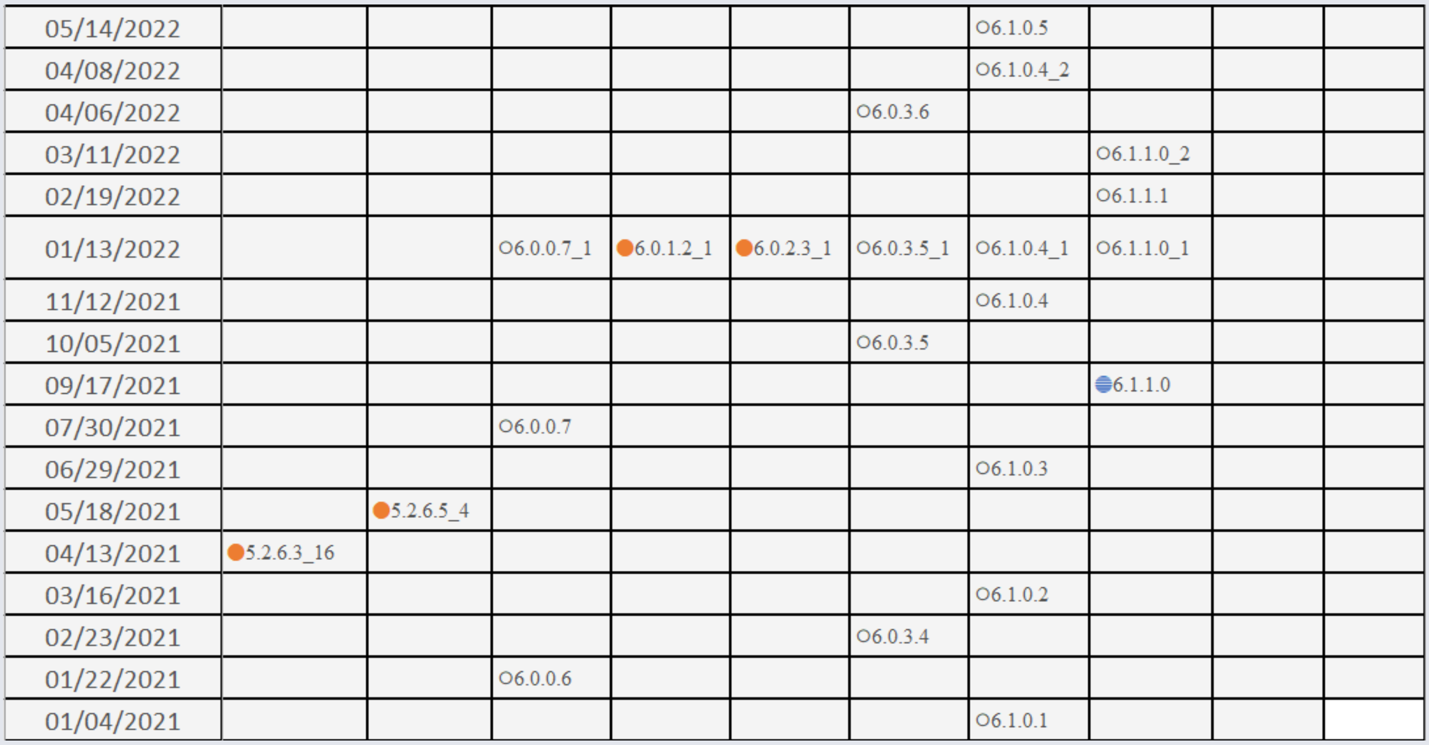
Modified date: 07 May 2024

IBM B2B Integrator / IBM Sterling File Gateway. Releases dates.

The following Timeline Illustration shows the release dates of the various IBM B2B Integrator or IBM Sterling File Gateway releases:

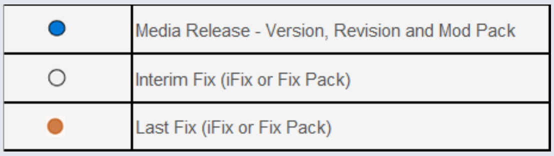


Dates/Releases	5.2.6.3	5.2.6.5	6.0.0.0	6.0.1.0	6.0.2.0	6.0.3.0	6.1.0.0	6.1.1.0	6.1.2.0	6.2.0.0
04/05/2024										○6.2.0.1
02/16/2024									○6.1.2.5	
11/17/2023						●6.0.3.9				
10/06/2023							○6.1.0.8			
09/22/2023										◍6.2.0.0
07/25/2023									○6.1.2.3	
06/08/2023								●6.1.1.4		
04/14/2023							○6.1.0.7			
03/09/2023									○6.1.2.2	
02/07/2023						○6.0.3.8				
12/24/2022								○6.1.1.3		
12/23/2022									○6.1.2.1	
10/28/2022							○6.1.0.6			
09/22/2022						○6.0.3.7				
09/05/2022							○6.1.0.5_2			
08/11/2022								○6.1.1.2		
07/21/2022									◍6.1.2.0 (does not include 6008)	
07/14/2022							○6.1.0.5_1			
07/11/2022						○6.0.3.6_1				
06/20/2022			○6.0.0.8							



05/14/2022							○6.1.0.5			
04/08/2022							○6.1.0.4_2			
04/06/2022						○6.0.3.6				
03/11/2022								○6.1.1.0_2		
02/19/2022								○6.1.1.1		
01/13/2022			○6.0.0.7_1	🟠6.0.1.2_1	🟠6.0.2.3_1	○6.0.3.5_1	○6.1.0.4_1	○6.1.1.0_1		
11/12/2021							○6.1.0.4			
10/05/2021						○6.0.3.5				
09/17/2021								🔵6.1.1.0		
07/30/2021			○6.0.0.7							
06/29/2021							○6.1.0.3			
05/18/2021		🟠5.2.6.5_4								
04/13/2021	🟠5.2.6.3_16									
03/16/2021							○6.1.0.2			
02/23/2021						○6.0.3.4				
01/22/2021			○6.0.0.6							
01/04/2021							○6.1.0.1			

Legend



🔵	Media Release - Version, Revision and Mod Pack
○	Interim Fix (iFix or Fix Pack)
🟠	Last Fix (iFix or Fix Pack)

Troubleshooting

IBM Sterling Control Center Monitor.

Control Center reporting Connect:Direct Server is down.

Troubleshooting

Problem

Connect:Direct UNIX and Connect:Direct Windows server reporting CCTR034E Server Down in Control Center alerts.

Symptom

Sterling Control Center engine log shows a sequence of error message for the Connect Direct Server;

CNCD058E Error getting data from server

CNCD049E Server Task error

CNCD024E Error getting stats from server.

Cause

The value for **tcp.api.inactivity.timeout** in Connect Direct was set too low.

Diagnosing The Problem

Review the Control Center Engine Logs and the Connect Direct value for tcp.max.time.to.wait

Resolving The Problem

Check the "Monitor Rest Time" in Control Center under the CD Server properties.

Verify that the CD "tcp.api.inactivity.timeout" value is set higher than the Monitor Rest Time in Control Center.

Related Information

IBM Sterling Connect:Direct Local Node Parameters

Communication

If you need more information about any of the contents of our newsletter, please do not hesitate to contact us. We will be happy to answer your questions

info@b2b.solutions