

# Integration News

T2 2024

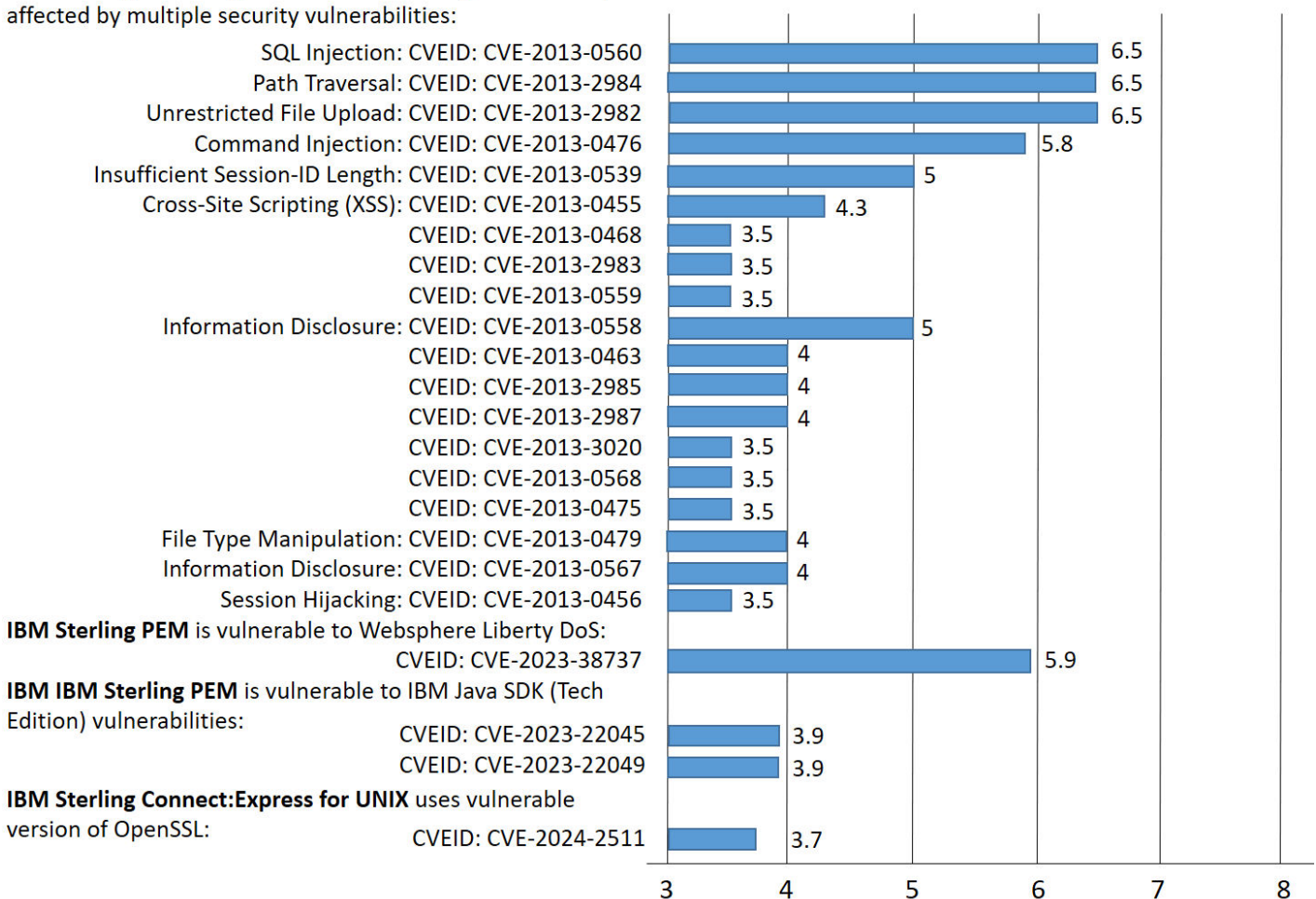


In this issue:

## IBM Sterling B2B Data Exchange Solutions. SECURITY NEWS:

**IBM Sterling B2B Integrator** and **IBM Sterling File Gateway** are affected by multiple security vulnerabilities:

Vulnerability mapping base score



### Other contents:

- What's new in **IBM Sterling B2B Integrator 6.2.0.2**
- Troubleshooting. An attempt to edit a Service or Adapter in a **Sterling B2B Integrator** instance running in an OCP environment times out after 60 seconds
- Fix List for **IBM Sterling B2B Integrator V6.2.0.2**
- **IBM Sterling B2B Integrator/Global Mailbox** Components Versions.
- Troubleshooting. IBM Sterling B2B Integrator 6.1.x upgrade access to Queue Watcher is failing



## Vulnerabilities in IBM Sterling B2B Integrator and IBM Sterling File Gateway

### Summary

IBM Sterling B2B Integrator and IBM Sterling File Gateway are affected by multiple security vulnerabilities:

- SQL Injection
- Path Traversal
- Unrestricted File Upload
- Cross-Site Scripting (XSS)
- Insufficient Session-ID Length
- Information Disclosure
- Command Injection
- File Type Manipulation
- Session Hijacking

### Vulnerability Details

#### SQL Injection

**CVEID:** [CVE-2013-0560](#)

**Description:** IBM Sterling B2B Integrator and IBM Sterling File Gateway are subject to SQL Injection. An authenticated remote attacker could send specially-crafted SQL statements to various screens, which could allow the attacker to view, add, modify or delete information in the back-end database.

CVSS Base score: 6.5

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(AV:N/AC:L/AU:S/C:P/I:P/A:P)

#### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

#### Path Traversal

**CVEID:** [CVE-2013-2984](#)

**Description:** Path traversal is possible in IBM Sterling B2B Integrator and IBM Sterling File

Gateway. Successful attacker could gain access to restricted files.

CVSS Base score: 6.5

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(AV:N/AC:L/Au:S/C:P/I:P/A:P)

#### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2 and 5.1
IBM Sterling File Gateway	2.2 and 2.1

#### Unrestricted File Upload

**CVEID:** [CVE-2013-2982](#)

**Description:** Any type of file is allowed to be uploaded in IBM Sterling B2B Integrator and IBM Sterling File Gateway. Successful attacker could take advantage of the flaw to launch other attacks.

CVSS Base score: 6.5

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(AV:N/AC:L/AU:S/C:P/I:P/A:P)

#### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2 and 5.1
IBM Sterling File Gateway	2.2 and 2.1

#### Command Injection

**CVEID:** [CVE-2013-0476](#)

**Description:** IBM Sterling B2B Integrator and IBM Sterling File Gateway are vulnerable to FTP command injection attacks. A remote attacker could inject unauthorized FTP commands which could compromise the server.

CVSS Base score: 5.8

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(AV:N/AC:M/Au:N/C:P/I:P/A:N)

### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

#### Insufficient Session-ID Length

**CVEID:** [CVE-2013-0539](#)

**Description:** IBM Sterling B2B Integrator and IBM Sterling File Gateway are affected by an insufficient Session-ID length vulnerability that exists in a third party component. A shorter session identifier leaves the applications open to brute-force session guessing attacks. An attacker can hijack a user's session if the user's session identifier is guessed.

CVSS Base score: 5

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(AV:N/AC:L/AU:N/C:P/I:N/A:N)

#### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

#### Cross-Site Scripting (XSS)

**CVEID:** [CVE-2013-0455](#)

**Description:** Cross-Site Scripting (XSS) vulnerability is found in various areas of IBM Sterling B2B Integrator and IBM Sterling File Gateway. A remote attacker could exploit this vulnerability to execute a script in a victim's web browser within the security context of the hosting web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.



CVSS Base score: 4.3  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

**CVEID:** [CVE-2013-0468](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

**CVEID:** [CVE-2013-2983](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

**CVEID:** [CVE-2013-0559](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:N/AU:S/C:N/I:P/A:N)

**Affected Products and Versions**

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

**Information Disclosure**

**CVEID:** [CVE-2013-0558](#)

**Description:** Information Disclosure vulnerability is found in various areas of IBM Sterling B2B Integrator and IBM Sterling File Gateway. A remote attacker could exploit this vulnerability to gain insight into application implementation details to form further attacks.

CVSS Base score: 5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/AU:N/C:P/I:N/A:N)

**CVEID:** [CVE-2013-0463](#)

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

**CVEID:** [CVE-2013-2985](#)

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

**CVEID:** [CVE-2013-2987](#)

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

**CVEID:** [CVE-2013-3020](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:L/AC:M/Au:S/C:P/I:N/A:N)

**CVEID:** [CVE-2013-0568](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:S/C:P/I:N/A:N)

**CVEID:** [CVE-2013-0475](#)

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/Au:S/C:P/I:N/A:N)

**Affected Products and Versions**

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

**In File Type Manipulation**

**CVEID:** [CVE-2013-0479](#)

**Description:** IBM Sterling B2B Integrator and IBM Sterling File Gateway is vulnerable to file type or extension manipulation which could cause improper handling of the file.

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

**CVEID:** [CVE-2013-0479](#)

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

**Affected Products and Versions**

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0

**Information Disclosure**

**CVEID:** [CVE-2013-0567](#)

**Description:** Information Disclosure vulnerability is found in various areas of IBM Sterling File Gateway. A remote attacker could exploit this vulnerability to gain insight into application implementation details to form further attacks.

CVSS Base score: 4  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

**Affected Products and Versions**

Affected Product(s)	Version(s)
IBM Sterling File Gateway	2.2 and 2.1

**Session Hijacking**

**CVEID:** [CVE-2013-0456](#)

**Description:** The Sterling solutions are vulnerable to session hijacking through cookie path manipulation.

CVSS Base score: 3.5  
 CVSS Temporal Score: [Click here.](#)  
 CVSS Vector:  
 (AV:N/AC:M/AU:S/C:N/I:P/A:N)

**Affected Products and Versions**

Affected Product(s)	Version(s)
IBM Sterling B2B Integrator	5.2, 5.1 and 5.0
IBM Sterling File Gateway	2.2, 2.1 and 2.0



## Remediation/Fixes

Product	APAR	Remediated Fixes
IBM Sterling B2B Integrator 5.0 or IBM Sterling File Gateway 2.0	IC90773, IC92007, IC89294, IC89538, IC89434, IC89385, IC89429, IC86096, IC87672, IC88970, IC87731, IC89293, IC89291, IC88972, IC90483, IC92612, IC91628, IC92259	For the APAR fixes listed, apply Fix Pack 5010 available on <a href="#">IWM</a>
IBM Sterling B2B Integrator 5.1 or IBM Sterling File Gateway 2.1.	IC90773, IC91071, IC91046, IC89291, IC89293, IC89292, IC89295, IC88970, IC89429, IC89385, IC89434, IC90518, IC91012, IC91045, IC92888, IC84082, IC87731, IC87672, IC89538, IC86096, IC89294, IC90483, IC88972, IC91442, IC91525, IC92272, IC92007, IC91044, IC91151, IC94320, IC92259	For the APAR fixes listed, apply generic iFix 5104_1 available on <a href="#">IWM</a>
IBM Sterling B2B Integrator 5.2 or IBM Sterling File Gateway 2.2	IC90773, IC91071, IC91046, IC89291, IC89293, IC89292, IC89295, IC88970, IC89429, IC89385, IC89434, IC90518, IC91012, IC91045, IC92888, IC84082, IC87731, IC87672, IC89538, IC86096, IC89294, IC90483, IC88972, IC91442, IC91525, IC92272, IC92007, IC91044, IC91151, IC94320, IC92259	For the APAR fixes listed, apply generic iFix 5020401_3 available on <a href="#">Fix Central</a>
IBM Sterling B2B Integrator 5.2 or IBM Sterling File Gateway 2.2	IC90773, IC91071, IC91046, IC89291, IC89293, IC89292, IC89295, IC88970, IC89429, IC89385, IC89434, IC90518, IC91012, IC91045, IC92888, IC84082, IC87731, IC87672, IC89538, IC86096, IC89294, IC90483, IC88972, IC91442, IC91525, IC92272, IC92007, IC91044, IC91151, IC94320, IC92259	For the APAR fixes listed, apply Fix Pack 5020402 available on <a href="#">Fix Central</a>
IBM Sterling B2B Integrator 5.2 or IBM Sterling File Gateway 2.2	IC95996, IC88973	Apply 5020500 Fix Pack or Media available on <a href="#">Fix Central</a> and <a href="#">Passport Advantage</a> respectively

### Additional Information:

The iFixes listed above for Sterling B2B Integrator and Sterling File Gateway also contains fixes for the following reported vulnerabilities.

Title	CVE ID	Link
Improper validation of user supplied input on select IBM Sterling B2B Integrator screens	CVE-2012-5766	<a href="https://www.ibm.com/support/pages/apar/IC84082">https://www.ibm.com/support/pages/apar/IC84082</a>
IBM Sterling B2B Integrator's session or sensitive cookies do not have the secure attribute enabled	CVE-2012-5936	<a href="http://www.ibm.com/support/docview.wss?uid=swg21627985">http://www.ibm.com/support/docview.wss?uid=swg21627985</a>
Error in IBM Sterling B2B Integrator console processing could result in stack traces being displayed in the response	CVE-2013-0481	<a href="http://www.ibm.com/support/docview.wss?uid=swg21627986">http://www.ibm.com/support/docview.wss?uid=swg21627986</a>
A number of security vulnerabilities have been discovered in the OpenSSL libraries included in IBM Sterling B2B Integrator and IBM Sterling File Gateway.	Mutliple CVEs	<a href="http://www.ibm.com/support/docview.wss?uid=swg21640831">http://www.ibm.com/support/docview.wss?uid=swg21640831</a>

### Workarounds and Mitigations

None Known.





IBM Sterling Partner Engagement Manager is vulnerable to Websphere Liberty DoS

### Summary

IBM WebSphere Application Server Liberty 22.0.0.13 through 23.0.0.7 is vulnerable to a denial of service, caused by sending a specially-crafted request. IBM Sterling Partner Engagement Manager 6.2.3.1 has included an upgraded version of WebSphere Liberty, which remediates this vulnerability.

### Vulnerability Details

**CVEID:** [CVE-2023-38737](#)

**Description:** IBM WebSphere Application Server Liberty 22.0.0.13 through 23.0.0.7 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 262567.

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:N/I:N/A:H)

### Affected Products and Versions

Affected Product(s)	Version(s)
PEM	6.2.1
	6.2.2
	6.1.2
	6.2.3
	6.2.0

### Remediation/Fixes

Product	Version(s)	Remediation/Fix/Instructions
IBM Sterling Partner Engagement Manager Essentials Edition	6.2.3.1, 6.1.2.10, 6.2.0.8	<a href="#">Download 6.2.3.1 and follow installation instructions</a>

### Workarounds and Mitigations

None Known.



IBM Sterling Partner Engagement Manager is vulnerable to IBM Java SDK (Tech Edition) vulnerabilities

### Summary

IBM Sterling Partner Engagement Manager 6.2.3.1, 6.1.2.10, and 6.2.0.8 address IBM Java SDK (Tech Edition) CPU vulnerabilities attached to this Security Bulletin.

### Vulnerability Details

**CVEID:** [CVE-2023-22045](#)

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

CVSS Base score: 3.7

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

**CVEID:** [CVE-2023-22049](#)

**Description:** An unspecified vulnerability in Java SE related to the Libraries component could allow a remote attacker to cause low integrity impacts.

CVSS Base score: 3.7

CVSS Temporal Score: [Click here.](#)

CVSS Vector:

(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

### Affected Products and Versions

Affected Product(s)	Version(s)
PEM	6.2.1
	6.2.2
	6.1.2
	6.2.3
	6.2.0

### Remediation/Fixes

Product	Version(s)	Remediation/Fix/Instructions
IBM Sterling Partner Engagement Manager Essentials Edition	6.2.3.1, 6.1.2.10, 6.2.0.8	<a href="#">Download 6.2.3.1 and follow installation instructions</a>

### Workarounds and Mitigations

There are some temporary workarounds/mitigations that can be performed (see Oracle's Security Alert for more information), but they are not recommended as long-term solutions to this problem. Upgrading to the latest Partner Engagement Manager in your release is the only viable long-term solution.



IBM Sterling Connect:Express for UNIX uses vulnerable version of OpenSSL

### Summary

IBM Sterling Connect:Express for UNIX uses a version OpenSSL which is vulnerable to denial of service (CVE-2024-2511). This issue has been addressed by upgrading the version of OpenSSL.

### Vulnerability Details

**CVEID:** [CVE-2024-2511](#)

**Description:** OpenSSL is vulnerable to a denial of service, caused by improper server configuration validation. By using a specially crafted server configuration, a remote attacker could exploit this vulnerability to cause unbounded memory growth, and results in a denial of service condition.

CVSS Base score: 3.7

CVSS Temporal Score: [Click here.](#)



CVSS Vector:  
(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

### Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Express for UNIX	1.5.0.16190 and prior

### Workarounds and Mitigations

None.



What's new in IBM Sterling B2B Integrator 6.2.0.2

Last Updated: 2024-06-06

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

### New features

Following new features are introduced in this release:

- TLSv1.3 can now be configured for Kafka Services and Adapters. For more information, see:
  - [Kafka Client Adapter](#),
  - [Kafka Begin Session Service](#),
  - [Kafka Consumer Streams Adapter](#).
- Certified Container enhancements: The default start-up probe time intervals are now increased. For details, see [Configuring the Certified Container](#).

### Stack updates

**Note:** This Fix pack also includes security fixes and stack upgrades from release [6201](#)

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

- Amazon Ion - 1.5.1
- Apache Mina SSHD Common 2.12.1

- Amazon Ion - 1.5.1
- Apache Mina SSHD Common -
- CKEditor - 4.23
- Commons-codec - 1.15
- Commons-compress jar - 1.26.1
- Commons-net.jar - 3.9.0
- Esapi .jar - 2.5.2.0
- Google guava - 32.0.1 jre
- Jackson-annotate, Jackson-core, Jackson-databind and Jackson-dataformat-yaml - 2.16.1
- Jetty - 9.4.54
- Json-path - 2.9.0.jar
- Liberty server - 24.0.0.4
- Netty jars - 4.1.108
- Nimbus-jose-jwt - 9.37.2
- Spring-security jars - 5.8.11
- Spring-web - 5.3.33

For more information, see [Software Product Compatibility Report](#).



**Troubleshooting**  
An attempt to edit a Service or Adapter in a SB2BI instance running in an OCP environment times out after 60 seconds

### Problem

An attempt to edit a Service or Adapter in a Sterling B2B Integrator instance running in an OCP environment times out after 60 seconds or displays a blank screen

### Cause

Settings in centralops.properties.in require modification

### Environment

Red Hat OCP

### Diagnosing The Problem

Attempt to edit a Service or Adapter in a Sterling B2B Integrator instance running in an OCP environment. If the display shows only a blank screen or there is a timeout, the

centralops.properties.in file may require modification.

### Resolving The Problem

- Copy the [centralops.properties.in](#) from m ASI pod's /ibm/b2bi/install/properties/ to outside the pod.
- Copy the [centralops.properties.in](#) to the <SI\_CHARTS>/properties folder
- Edit the file and update **updateAllNodesInfo=true**
- Perform a helm upgrade and restart all pods.



**Fix List for Sterling B2B Integrator V6.2.0.2 and V6.2.0.3.**

This page contains comprehensive fix information for all Fix Packs released for Sterling B2B Integrator and Sterling File Gateway V6.2.0.2 and V6.2.0.3.

### 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:

1. Download the fix pack from Fix Central.
2. 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 (v6.2.0.2)

Link	Date Released	Status
<a href="#">Download</a>	June 04, 2024	Available

### Security Fixes

APAR	Description
IT45621	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45619	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46060	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
<a href="#">IT45707</a>	B2B API OF IBM STERLING B2B INTEGRATOR IS VULNEARBLE TO DENIAL OF SERVICE DUE TO JSON-PATH (CVE-2023-51074)
IT45690	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46040	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46041	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45722	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45949	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46024	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45998	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45623	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46036	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46059	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45620	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43937	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45982	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43979	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46050	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45596	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT45595	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46124	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46122	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46123	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46126	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

### Regular Fixes

APAR	Description
<a href="#">IT45854</a>	B2BI 6.2 - BEHAVIOR CHANGE IN THE 'PAGER' FIELD OF THE USER ACCOUNTS
<a href="#">IT45736</a>	STORED XSS ON QUEUEWATCHER UI AFTER MODIFYING PROPERTIES FILE
<a href="#">IT45850</a>	SANDBOX BUILD FAILS ON CATAMOUNT_BUILD_6020000_BRANCH
<a href="#">IT45808</a>	UPGRADE FROM 6114 TO 6201 FAILS WHEN FIPS MODE IN ENABLED
<a href="#">IT46015</a>	GLOBAL MAILBOXING INSTALLATION INTO B2BI FAILED TO IMPORT SERVICE INSTANCES
<a href="#">IT44945</a>	SFG 6.2 CHINESE DISPLAY HAS GARBLED CHARACTERS
<a href="#">IT45837</a>	FAILURE TO CREATE DUMMY IFIX FOR 6201
<a href="#">IT45622</a>	GETTING EXCEPTION ERROR UNMARSHALLING RETURN; NESTED EXCEPTION IS: JAVA.IO.EOFEXCEPTION IN FSA WITH SI 6.2

### Fix Pack (v6.2.0.3)

Link	Date Released	Status
<a href="#">Download</a>	September 02, 2024	Current

### Security Fixes

APAR	Description
IT46478	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46396	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46254	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)



APAR	Description
IT46103	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46083	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46084	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46358	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46411	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46353	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46100	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT43979	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46567	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46458	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44306	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44440	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46606	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44314	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46388	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46193	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46252	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46706	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46710	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46739	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46705	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46745	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46744	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46743	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT44303	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46746	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46709	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)
IT46742	DESCRIPTION IS NOT AVAILABLE (SECURITY/INTEGRITY ISSUE)

### Regular Fixes

APAR	Description
IT46207	HTML CODE APPEARS WHEN ADDING NEW OUTBOUND TP GROUP OR TRANSACTION ENVELOPE
IT46318	XMLTOJSONTRANSFORMER ERRORS AFTER UPGRADE TO 6.2.0.1
IT46304	PROBLEMS RESULT FROM THE DIFFERENCE BETWEEN CREATING SFG PARTNER IN SFG GUI VS. USE OF CREATE TRADING PARTNER REST API
IT46496	DOCUMENTATION ABOUT SUPPORTED HOST AND PUBLIC KEY TYPE ALGORITHMS AND OTHER SUPPORTED CIPHER/MAC/ALGOS FOR SFTP CONNECTIVITY
IT46519	IMPLEMENT AND TEST TLS 1.3 SUPPORT FOR CD REQUESTER ADAPTER (CDRA)
IT46215	FRESH INSTALL OF 6021 WITH FIPS ON FAILED
IT46453	NEW INSTALL OF 6.2 ON WINDOWS SERVER 2022 TO SQL SERVER 2022 WILL NOT COMPLETE START UP
IT46519	TLS 1.3 FOR CD REQUESTOR ADAPTER
IT46568	"KB DEBUG NEW CODE IN PLACE" IN EXTPURGE_EXE.LOG
IT46134	MYFILEGATEWAY2.0 UI - ERRORS WHILE ACCESSING MAILBOXES
IT46165	SUPPORT FOR KEY_NEW_PATH IN ONPUTAFTEREXECUTE SFTP 2.0 USER EXIT FOR INTERNAL RENAMING A FILE AFTER PUT OPERATION
IT44592	HISTORICAL: BP WITH DOCUMENT STORAGE SET TO 'FILE SYSTEM' OR 'OBJECT STORE' NOT GETTING RETAINED DURING UPGRADE AND DOCUMENT STORAGE APPEARS AS BLANK FOR THE BPs
IT46589	SENDERSESSIONID IS NOT CREATED IN PROCESSDATA WHEN SNODEID CONTAINS ONLY THE USER NAME
IT46228	WINCONVERT.SH IS NOT CONVERTING A GENTRAN SERVER WINDOWS PARTNER FILE INTO AN XML RESOURCE FILE TO IMPORT INTO B2BI
IT46488	WHEN UPDATING PERMISSIONS IN B2BI, ONLY UNIQUE NAMES SHOULD BE USED
IT46505	B2BI CONTAINER 6.2.0.1 HELM CHART ISSUE : DUPLICATE ENVIRONMENT VARIABLE
IT46349	ERROR WHEN CREATING / IMPORTING SSH USER IDENTITY KEY AND SSH HOST IDENTITY KEY





APAR	Description
IT46643	TRYING TO GRAB SSH KNOWN HOST KEY IN B2Bi 6.2.0.2 FAILS WITH JAVA.LANG.NOSUCHMETHODERROR: ORG/APACHE/SSHD/CLIENT/FUTURE/CONNECTFUTURE.AWAIT(J)Z
IT46378	H005 ORDER TYPES ARE NOT DISPLAYED CORRECTLY WHEN CREATING A NEW OFFER



## IBM Sterling B2B Integrator/Global Mailbox Components Versions.

### Detailed System Requirements

#### Abstract

Refer to the below table to determine which version of Apache Cassandra, Apache ZooKeeper, Reaper for Apache Cassandra, or WebSphere Application Server Liberty comes with your IBM Sterling B2B Integrator/Global Mailbox fix pack.

#### Content:

IBM Sterling B2Bi/GM Fix Pack Version	Apache Cassandra Version	Apache ZooKeeper Version	Reaper for Apache Cassandra Version	WebSphere Application Server Liberty Version
<b>6.0.3.x</b>				
6.0.3.3	3.11.0	3.5.5	1.1.0	20.0.0.9
6.0.3.4	3.11.0	3.5.5	1.1.0	20.0.0.12
6.0.3.5	3.11.0	3.5.5	1.1.0	21.0.0.6
6.0.3.6	3.11.0	3.5.5	1.1.0	21.0.0.6
6.0.3.7	3.11.0	3.5.5	1.1.0	22.0.0.5
6.0.3.8	3.11.0	3.5.5	1.1.0	22.0.0.13
6.0.3.9	3.11.0	3.5.5	1.1.0	23.0.0.9
<b>6.1.0.x</b>				
6.1.0.0	3.11.6	3.5.5	1.1.0	20.0.0.5
6.1.0.1	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.2	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.3	3.11.6	3.5.5	1.1.0	20.0.0.12
6.1.0.4	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.4_1	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.4_2	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.5	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.5_2	3.11.6	3.5.5	1.1.0	21.0.0.6
6.1.0.6	3.11.6	3.5.5	1.1.0	22.0.0.5
6.1.0.7	3.11.6	3.5.5	1.1.0	22.0.0.13
<b>6.1.1.x</b>				
6.1.1.0	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.0_1	3.11.10	3.6.3	2.3.1	21.0.0.6



IBM Sterling B2Bi/GM Fix Pack Version	Apache Cassandra Version	Apache ZooKeeper Version	Reaper for Apache Cassandra Version	WebSphere Application Server Liberty Version
6.1.1.1	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.2	3.11.10	3.6.3	2.3.1	21.0.0.6
6.1.1.3	3.11.10	3.6.3	2.3.1	22.0.0.10
6.1.1.4	3.11.10	3.6.3	2.3.1	23.0.0.3
<b>6.1.2.x</b>				
6.1.2.0	3.11.10	3.6.2	2.3.1	21.0.0.3
6.1.2.1	4.0.6	3.8.0	3.2.0	22.0.0.10
6.1.2.2	4.0.7	3.8.0	3.2.1	22.0.0.13
6.1.2.3	4.0.10	3.8.1	3.3.1	23.0.0.4
6.1.2.5	4.0.10	3.9.1	3.3.1	23.0.0.11
<b>6.2.0.x</b>				
6.2.0.0	4.0.10	3.8.1	3.3.1	23.0.0.4
6.2.0.1	4.0.10	3.9.1	3.3.1	23.0.0.12
6.2.0.2	4.0.10	3.9.1	3.3.1	23.0.0.4
6.2.0.3	4.0.13	3.9.1	3.6.0	24.0.0.7



### Troubleshooting

IBM Sterling B2B Integrator 6.1.x upgrade access to Queue Watcher is failing

#### Problem

Queue Watcher log on fails after upgrading IBM Sterling B2B Integrator

#### Symptom

After logging on receive error "This site can't provide a secure connection ERR\_SSL\_PROTOCOL\_ERROR."

#### Cause

The URL had change from HTTP to HTTPS but the port was still the non-secure port.

The noapp.SKIP\_BASEPORT\_DEPLOYMENT\_WARS and noapp.HTTPS\_REDIRECT\_WARS did not include queueWatch.

```
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
```

```
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
```

The HTTP server adapter did not have the war file for the Queue Watcher deployed.

#### Diagnosing The Problem

1. Review the URL and error messages.
2. Review customer override properties.
3. Review HTTP server adapter definitions.

#### Resolving The Problem

Update the properties to include the Queue Watcher  
noapp.SKIP\_BASEPORT\_DEPLOYMENT\_WARS=admin,dashboard,gbm,

communitymanagement,myaft,portlets,mailbox,queueWatch

Deployed Queue Watcher on the correct HTTP Server adapter.

#### Related Information

[Accessing Queue Watcher](#)  
[Enable Auto-Redirect to HTTPS](#)

#### 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