B2B Solutions
Let's build IT together

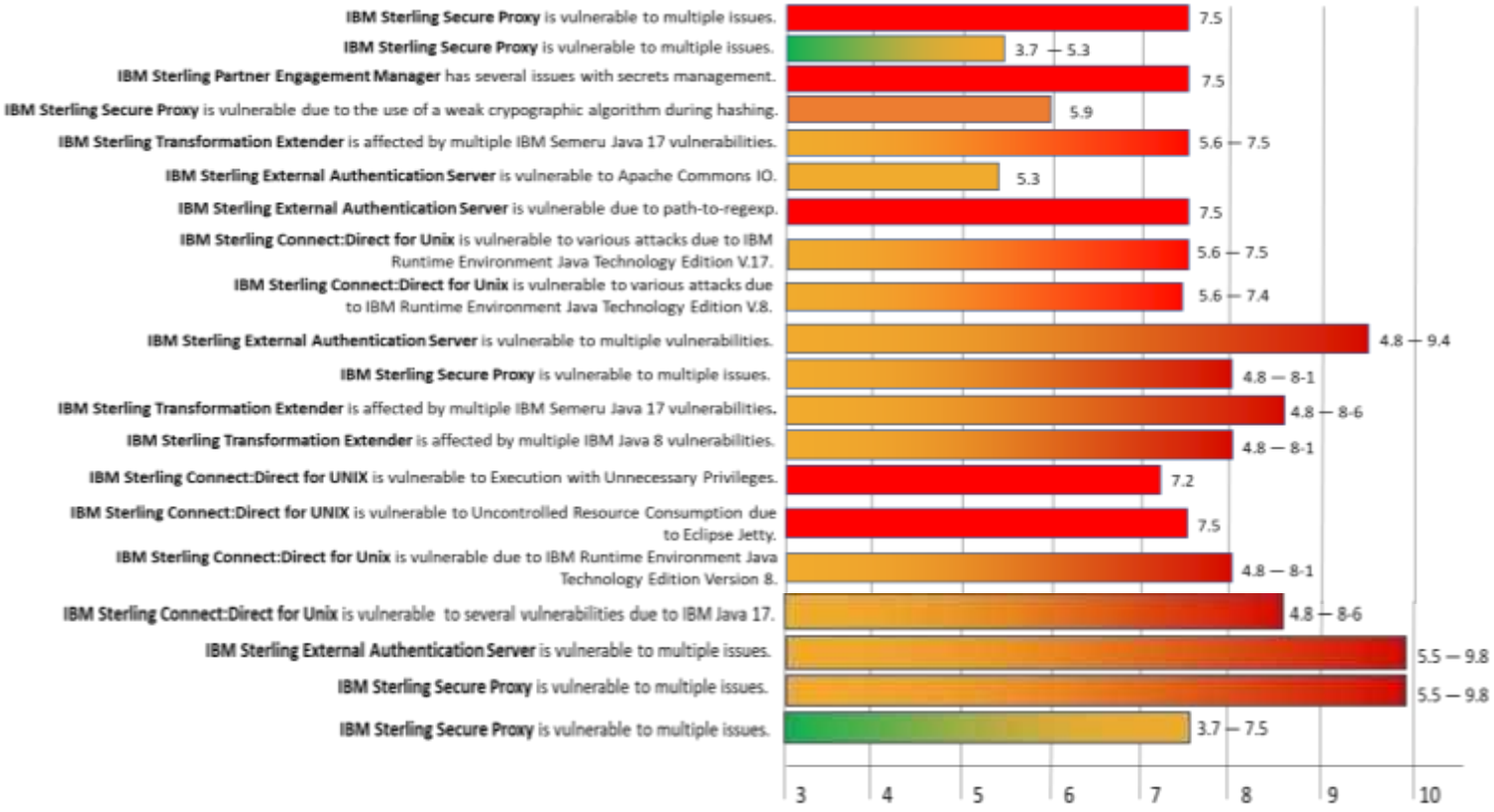
Integration News

T3 2025

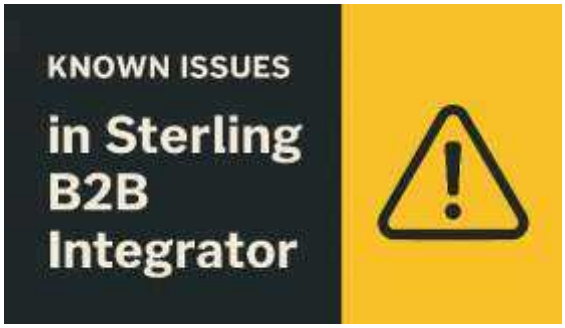
In this issue:

IBM Sterling B2B Data Exchange Solutions. SECURITY NEWS:

Vulnerability mapping base score



Other Contents:



IBM Sterling Secure Proxy is vulnerable to multiple issues.

Summary

Multple vulnerabilities affect IBM Sterling Secure Proxy and are addressed in the latest release and iFix.

Vulnerability Details

CVEID: CVE-2024-29857

Description: The Bouncy Castle Crypto Package for Java is vulnerable to a denial of service, caused by improper input validation. By importing an EC certificate with crafted F2m parameters, a remote attacker could exploit this vulnerability to cause excessive CPU consumption.

CWE: CWE-125: Out-of-bounds Read

CVSS Source: IBM X-Force
CVSS Base score: 7.5
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 Secure Proxy	6.1.0.0 6.1.0.1
IBM Sterling Secure Proxy	6.2.0.0 6.2.0.1

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.1.0.0 6.1.0.1	6.1.0.1 iFix 03 Fix Central
	6.2.0.0 6.2.0.1	6.2.0.1 iFix 02 Fix Central

Workarounds and Mitigations

None.

Change History

28 Feb 2025: Initial Publication

IBM Sterling Secure Proxy is vulnerable to multiple issues.

Summary

Multple vulnerabilities affect IBM Sterling Secure Proxy. They are addressed in the latest release and iFix.

Vulnerability Details

CVEID: CVE-2024-21235

Description: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to accessible data as well as unauthorized read access to a subset of accessible data.
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21217

Description: Vulnerability in Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CWE: CWE-502: Deserialization of Untrusted Data

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21210

Description: Vulnerability in Java SE (component: Hotspot). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some accessible data.

CWE: CWE-203: Observable Discrepancy

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-21208

Description: Vulnerability in Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS).

CWE: CWE-203: Observable Discrepancy

CVSS Source: Oracle
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-10917

Description: In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.

CWE: CWE-190: Integer Overflow or Wraparound
CVSS Source: NVD
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.0.0.0 6.0.3.1
IBM Sterling Secure Proxy	6.1.0.0 6.1.0.1
IBM Sterling Secure Proxy	6.2.0.0 6.2.0.1

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.0.0.0 6.0.3.1	6.0.3.1 iFix 03 Fix Central
	6.1.0.0 6.1.0.1	6.1.0.1 iFix 03 Fix Central
	6.2.0.0 6.2.0.1	6.2.0.1 iFix 02 Fix Central

Workarounds and Mitigations
None.

Change History
15 Apr 2025: Initial Publication

IBM Sterling Partner Engagement Manager has several issues with secrets management

Summary

IBM Sterling Partner Engagement Manager's JWT secret is stored in public Helm Charts and is not stored as a Kubernetes secret. This issue has been addressed in the latest Helm Chart.

Vulnerability Details

CVEID: CVE-2025-33093
Description: IBM Sterling Partner Engagement Manager's JWT secret is stored in public Helm Charts and is not stored as a Kubernetes secret.
CWE: CWE-260: Password in Configuration File
CVSS Source: IBM
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
PEM	6.1.x
PEM	6.2.x

Remediation/Fixes

Product	Version	Remediation/Fix /Instructions
PEM	6.1.x, 6.2.0, 6.2.3, 6.2.4	6.2.0,6.2.3,6.2.4

Workarounds and Mitigations
None.

Change History
07 May 2025: Initial Publication

IBM Sterling Secure Proxy is vulnerable due to the use of a weak crypographic algorithm during hashing

Vulnerability Details

CVEID: CVE-2024-38341
Description: IBM Sterling Secure Proxy uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.
CWE: CWE-328: Use of Weak Hash
CVSS Source: IBM X-Force
CVSS Base score: 5.9
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 Secure Proxy	6.0.0.0 6.0.3.1
IBM Sterling Secure Proxy	6.1.0.0 6.1.0.1
IBM Sterling Secure Proxy	6.2.0.0 6.2.0.1

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.0.0.0 6.0.3.1	6.0.3.1 iFix 03 Fix Central
	6.1.0.0 6.1.0.1	6.1.0.1 iFix 03 Fix Central
	6.2.0.0 6.2.0.1	6.2.0.1 iFix 02 Fix Central

Workarounds and Mitigations
None.

Change History
28 May 2025: Initial Publication

IBM Sterling Transformation Extender is affected by multiple IBM Semeru Java 17 vulnerabilities

Summary

IBM Sterling Transformation Extender uses IBM Semeru Runtime Certified Edition, Version 17.

Vulnerability Details

CVEID: CVE-2025-21587
Description: An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2025-30698
Description: An unspecified

vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 5.6
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVEID: CVE-2025-2900
Description: IBM Semeru Runtime 8.0.302.0 through 8.0.442.0, 11.0.12.0 through 11.0.26.0, 17.0.0.0 through 17.0.14.0, and 21.0.0.0 through 12.0.6.0 is vulnerable to a denial of service caused by a buffer overflow and subsequent crash, due to a defect in its native AES/CBC encryption implementation.
CWE: CWE-122: Heap-based Buffer Overflow
CVSS Source: IBM
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:

CVEID: CVE-2025-4447
Description: In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.
CWE: CWE-121: Stack-based Buffer Overflow
CVSS Source: emo@eclipse.org
CVSS Base score: 7
CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Transformation Extender	11.0.1

Remediation/Fixes

Product	Version	APAR	Dow. URL
IBM Sterling Transformation Extender	11.0.1.1	PH67016	Link

Workarounds and Mitigations
None.

Change History
03 Jul 2025: Initial Publication

IBM Sterling External Authentication Server is vulnerable to Apache Commons IO

Summary
Security Bulletin:IBM Sterling External Authentication Server is vulnerable to Apache Commons IO.

Vulnerability Details

CVEID: CVE-2024-47554
Description: Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.
CWE: CWE-400: Uncontrolled Resource Consumption
CVSS Source: IBM X-Force
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.1/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 Secure External Authentication Server	6.0.X – 6.1.X

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Secure External Authentication Server	6.1.0.0 - 6.1.0.2	6.1.0.2 iFix 03 Fix Central
	6.0.3.0 - 6.0.3.1	6.0.3.1 iFix 03 Fix Central

Workarounds and Mitigations
None.

Change History
09 Jul 2025: Initial Publication

IBM Sterling External Authentication Server is vuulnerable due to path-to-regexp

Summary
IBM Sterling External Authentication Server uses the npm path-to-regexp, which is vulnerable to CVE-2024-45296.

Vulnerability Details
CVEID: CVE-2024-45296
Description: path-to-regexp turns path strings into a regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. Because JavaScript is single threaded and regex matching runs on the main thread, poor performance will block the event loop and lead to a DoS. The bad regular expression is generated any time you have two parameters within a single segment, separated by something that is not a period (.). For users of 0.1, upgrade to 0.1.10. All other users should upgrade to 8.0.0.
CWE: CWE-1333: Inefficient Regular Expression Complexity
CVSS Source: CVE.org
CVSS Base score: 7.5
CVSS Vector:

(CVSS:3.1/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 External Authentication Server	6.1.X

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling External Authentication Server	6.1.0.0 - 6.1.0.2	6.1.0.2 iFix 03 Fix Central

Workarounds and Mitigations
None.

Change History
09 Jul 2025: Initial Publication

IBM Sterling Connect:Direct for Unix is vulnerable to various attacks due to IBM Runtime Environment Java Technology Edition V.17

Summary
IBM Java 17 is used by IBM Sterling Connect:Direct for UNIX in product configuration and data transmission. IBM Sterling Connect:Direct for UNIX is impacted by vulnerabilities in IBM Java 17. IBM Sterling Connect:Direct for UNIX has upgraded IBM Java 17 to address the issues.

Vulnerability Details

CVEID: CVE-2025-21587
Description: An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2025-30698
Description: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 5.6
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVEID: CVE-2025-2900
Description: IBM Semeru Runtime 8.0.302.0 through 8.0.442.0, 11.0.12.0 through 11.0.26.0, 17.0.0.0 through 17.0.14.0, and 21.0.0.0 through 12.0.6.0 is vulnerable to a denial of service caused by a buffer overflow and subsequent crash, due to a defect in its native AES/CBC encryption implementation.
CWE: CWE-122: Heap-based Buffer Overflow
CVSS Source: Oracle
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2025-4447
Description: In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.
CWE: CWE-121: Stack-based Buffer Overflow
CVSS Source: Oracle
CVSS Base score: 7
CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for Unix	6.4.0.0 - 6.4.0.1.iFix036
	6.3.0.3 - 6.3.0.4.iFix033

Remediation/Fixes

Product	Version	Remediation/Fix /Instructions
IBM Sterling Connect: Direct for Unix	6.3.0	Apply 6.3.0.5, available on Fix Central.
	6.4.0	Apply 6.4.0.2, available on Fix Central.

Workarounds and Mitigations
None.

IBM Sterling Connect:Direct for Unix is vulnerable to various attacks due to IBM Runtime Environment Java Technology Edition V.8

Summary
IBM Java 8 is used by IBM Sterling Connect:Direct for UNIX in product configuration and data transmission. IBM Sterling Connect:Direct for UNIX is impacted by vulnerabilities in IBM Java 8. IBM Sterling Connect:Direct for UNIX has upgraded IBM Java 8 to address the issues.

Vulnerability Details

CVEID: CVE-2025-21587
Description: An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CWE: CWE-284: Improper Access Control

CVSS Source: Oracle
CVSS Base score: 7.4
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2025-30698
Description: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 5.6
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVEID: CVE-2025-4447
Description: In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.
CWE: CWE-121: Stack-based Buffer Overflow
CVSS Source: Oracle
CVSS Base score: 7
CVSS Vector:
(CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for Unix	6.2.0.0 - 6.2.0.7.iFix051

Remediation/Fixes

Product	Version	Remediation/Fix /Instructions
IBM Sterling Connect: Direct for Unix	6.2.0	Apply 6.2.0.7.iFix052, available on Fix Central.

Workarounds and Mitigations
None.

Change History
14 Jul 2025: Initial Publication

IBM Sterling External Authentication Server is vulnerable to multiple vulnerabilities

Summary
Multple vulnerabilities affect IBM Sterling External Authentication Server and are addressed in the latest fixpack

Vulnerability Details

CVEID: CVE-2025-7783
Description: Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. This issue affects form-data: < 2.5.4, 3.0.0 - 3.0.3, 4.0.0 - 4.0.3.
CWE: CWE-330: Use of Insufficiently Random Values
CVSS Source: Harborist
CVSS Base score: 9.4
CVSS Vector:
(CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N)

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java

applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30761
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling External Authentication Server	6.1.0.0 6.1.0.2
	6.1.1.0

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Secure External Authentication Server	6.1.0.0 6.1.0.2	6.1.0.3 GA Fix Central
	6.1.1.0	6.1.1.1 GA Fix Central

Workarounds and Mitigations
None.

Change History
19 Nov 2025: Initial Publication

IBM Sterling Secure Proxy is vulnerable to multiple issues

Summary
Multple vulnerabilities affect IBM Sterling Secure Proxy and are addressed in the latest fixpack

Vulnerability Details

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this

vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30761
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2025-7783
Description: Use of Insufficiently Random Values vulnerability in form-data allows HTTP

Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. This issue affects form-data: < 2.5.4, 3.0.0 - 3.0.3, 4.0.0 - 4.0.3.
CWE: CWE-330: Use of Insufficiently Random Values
CVSS Source: Harborist
CVSS Base score: 9.4
CVSS Vector: (CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.1.0.0 - 6.1.0.1
IBM Sterling Secure Proxy	6.2.0.0 - 6.2.0.1
IBM Sterling Secure Proxy	6.2.1.0

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.1.0.0 - 6.1.0.1	6.1.0.2 GA Fix Central
	6.2.0.0 - 6.2.0.1	6.2.0.2 GA Fix Central
	6.2.1.0	6.2.1.1 GA Fix Central

Workarounds and Mitigations
None.

Change History
17 Nov 2025: Initial Publication

IBM Sterling Transformation Extender is affected by multiple IBM Semeru Java 17 vulnerabilities

Summary
IBM Sterling Transformation Extender uses IBM Semeru Runtime Certified Edition, Version 17 and is affected by multiple vulnerabilities (CVE-2025-53057, CVE-2025-53066, CVE-2025-50059, CVE-2025-50106, CVE-2025-30749, CVE-2025-30761 and CVE-2025-30754).

Vulnerability Details

CVEID: CVE-2025-53057
Description: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause no confidentiality impact, high integrity impact, and no availability impact.
CVEID: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-53066
Description: An unspecified vulnerability in Java SE related to the JAXP component could allow a remote attacker to cause high confidentiality impact, no integrity impact, and no availability impact.
CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVSS Source: Oracle
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2025-50059
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 8.6
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition.

Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749

Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30761

Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754

Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Transformation Extender	11.0.1.1, 11.0.2.0

Remediation/Fixes

Product	Version	APAR / Download URL
IBM Sterling Transformation Extender	11.0.1.1	PH68819 / Link
	11.0.2.0	PH68819 / Link

Workarounds and Mitigations
None.

Change History
11 Nov 2025: Initial Publication

IBM Sterling Transformation Extender is affected by multiple IBM Java 8 vulnerabilities

Summary
IBM Sterling Transformation Extender uses IBM SDK, Java Technology Edition, Version 8 and is affected by multiple vulnerabilities.

Vulnerability Details

CVEID: CVE-2025-53066
Description: An unspecified vulnerability in Java SE related to the JAXP component could allow a remote attacker to cause high confidentiality impact, no integrity impact, and no availability impact.
CWE: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVSS Source: Oracle
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2025-53057
Description: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause no confidentiality impact, high integrity impact, and no availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE

(component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30761
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Transformation Extender	10.1.0.2, 10.1.1.1, 10.1.2.1, 11.0.0.0

Remediation/Fixes

Product	Version	APAR / Download URL
IBM Sterling Transformation Extender	10.1.0.2	PH68266 / Link
	10.1.1.1	PH68266 / Link
	10.1.2.1	PH68266 / Link
	11.0.0.0	PH68266 / Link

Workarounds and Mitigations
None.

Change History
11 Nov 2025: Initial Publication

IBM Sterling Connect:Direct for UNIX is vulnerable to Execution with Unnecessary Privileges.

Summary
IBM Sterling Control Center can apply maintenance to and upgrade IBM Sterling Connect:Direct for UNIX. The Control Center administrator has the option of running pre and post update scripts. Those scripts are run as root; they should be run as the standard user account under which Connect:Direct UNIX was installed.

CVEID: CVE-2025-36137
Description: IBM Sterling Connect:Direct for UNIX incorrectly assigns permissions for maintenance tasks to Control Center Director (CCD) users that could allow a privileged user to escalate their privileges further due to unnecessary privilege assignment for post update scripts.
CWE: CWE-250: Execution with Unnecessary Privileges
CVSS Source: IBM
CVSS Base score: 7.2
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.2.0.7 - 6.2.0.9.iFix004
	6.4.0.0 - 6.4.0.2.iFix001
	6.3.0.2 - 6.3.0.5.iFix002

Remediation/Fixes

Product	V.	Remediation/Fix/ Instructions
IBM Sterling Connect: Direct for UNIX	6.4.0	Apply 6.4.0.2.iFix004, available on Fix Central.
	6.3.0	Apply 6.3.0.5.iFix008, available on Fix Central.
	6.2.0	Apply 6.2.0.9.iFix005, available on Fix Central.

Workarounds and Mitigations
None.

Change History
30 Oct 2025: Initial Publication

IBM Sterling Connect:Direct for UNIX is vulnerable to Uncontrolled Resource Consumption due to Eclipse Jetty.

CVEID: CVE-2025-1948
Description: In Eclipse Jetty versions 12.0.0 to 12.0.16 included, an HTTP/2 client can specify a very large value for the HTTP/2 settings parameter SETTINGS_MAX_HEADER_LIST_SIZE. The Jetty HTTP/2 server does not perform validation on this setting, and tries to allocate a ByteBuffer of the specified capacity to encode HTTP responses, likely resulting in OutOfMemoryError being thrown, or even the JVM process exiting.
CWE: CWE-400: Uncontrolled Resource Consumption
CVSS Source: emo@eclipse.org
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/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 Connect:Direct for UNIX	6.4.0.0 - 6.4.0.2.iFix012
	6.3.0.0 - 6.3.0.5.iFix012

Remediation/Fixes

Product	V.	Remediation/Fix/ Instructions
IBM Sterling Connect: Direct for UNIX	6.4.0	Apply 6.4.0.3, available on Fix Central.
	6.3.0	Apply 6.3.0.6, available on Fix Central.

Workarounds and Mitigations
None.

Change History
01 Oct 2025: Initial Publication

IBM Sterling Connect:Direct for Unix is vulnerable due to IBM Runtime Environment Java Technology Edition Version 8.

Summary
IBM Java 8 is used by IBM Sterling Connect:Direct for UNIX in product configuration and data transmission. IBM Sterling Connect:Direct for UNIX is impacted by vulnerabilities in IBM Java 8. IBM Sterling Connect:Direct for UNIX has upgraded IBM Java 8 to address the issues.

Vulnerability Details

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start

applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30761
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector:
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.2.0.0 to 6.2.0.8.iFix004

Remediation/Fixes

Product	V.	Remediation/Fix/ Instructions
IBM Sterling Connect: Direct for UNIX	6.2.0	Apply 6.2.0.9, available on Fix Central.

Workarounds and Mitigations
None.

Change History
01 Oct 2025: Initial Publication

IBM Sterling Connect:Direct for Unix is vulnerable to several vulnerabilities due to IBM Java 17

Summary
IBM Java 17 is used by IBM Sterling Connect:Direct for UNIX in product configuration and data transmission. IBM Sterling Connect:Direct for UNIX is impacted by vulnerabilities in IBM Java 17. IBM Sterling Connect:Direct for UNIX has upgraded IBM Java 17 to address the issues.

Vulnerability Details

CVEID: CVE-2025-50059
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 8.6
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N)

CVEID: CVE-2025-50106
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-30749
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CVSS Source: Oracle
CVSS Base score: 8.1
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:

U/C:H/I:H/A:H)

CVEID: CVE-2025-30761
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: Oracle
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2025-30754
Description: Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Connect:Direct for UNIX	6.4.0.0 - 6.4.0.2.iFix012
	6.3.0.3 - 6.3.0.5.iFix012

Remediation/Fixes

Product	Version	Remediation /Fix/Instructions
IBM Sterling Connect: Direct for UNIX	6.3.0	Apply 6.3.0.6, available on Fix Central.
	6.4.0	Apply 6.4.0.3, available on Fix Central.

Workarounds and Mitigations
None.

Change History
01 Oct 2025: Initial Publication.

IBM Sterling External Authentication Server is vulnerable to multiple issues

Summary
Multple vulnerabilities affect IBM Sterling External Authentication Server and are addressed in the latest release and iFix.

Vulnerability Details

CVEID: CVE-2025-27152
Description: axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if baseURL is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.
CWE: CWE-918: Server-Side Request Forgery (SSRF)
CVSS Source: IBM
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2025-1470
Description: In Eclipse OMR, from

the initial contribution to version 0.4.0, some OMR internal port library and utilities consumers of z/OS atoe functions do not check their return values for NULL memory pointers or for memory allocation failures. This can lead to NULL pointer dereference crashes. Beginning in version 0.5.0, internal OMR consumers of atoe functions handle NULL return values and memory allocation failures correctly.
CWE: CWE-476: NULL Pointer Dereference
CVSS Source: NVD
CVSS Base score: 5.5
CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2025-1471
Description: In Eclipse OMR versions 0.2.0 to 0.4.0, some of the z/OS atoe print functions use a constant length buffer for string conversion. If the input format string and arguments are larger than the buffer size then buffer overflow occurs. Beginning in version 0.5.0, the conversion buffers are sized correctly and checked appropriately to prevent buffer overflows.
CWE: CWE-787: Out-of-bounds Write
CVSS Source: NVD
CVSS Base score: 7.8
CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2024-13009
Description: In Eclipse Jetty versions 9.4.0 to 9.4.56 a buffer can be incorrectly released when confronted with a gzip error when inflating a request body. This can result in corrupted and/or inadvertent sharing of data between requests.
CWE: CWE-404: Improper Resource Shutdown or Release
CVSS Source: emo@eclipse.org
CVSS Base score: 7.2
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)

CVEID: CVE-2025-21587
Description: An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2025-30698
Description: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle
VSS Base score: 5.6
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVEID: CVE-2025-4447
Description: In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.
CWE: CWE-121: Stack-based Buffer Overflow
CVSS Source: NVD
CVSS Base score: 9.8
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling External Authentication Server	6.1.0.x

Remediation/Fixes

Product	Version(s)	Fixed-in Version(s)/ Remediation /Fix
IBM Sterling External Authentication Server	6.1.0.x	6.1.0.3 GA / Fix Central

Workarounds and Mitigations
None.

Change History
28 Aug 2025: Initial Publication

IBM Sterling Secure Proxy is vulnerable to multiple issues.

Summary
Multple vulnerabilities affect IBM Sterling Secure Proxy and are addressed in the latest release and iFix.

Vulnerability Details

CVEID: CVE-2024-13009
Description: In Eclipse Jetty versions 9.4.0 to 9.4.56 a buffer can be incorrectly released when confronted with a gzip error when inflating a request body. This can result in corrupted and/or inadvertent sharing of data between requests.
CWE: CWE-404: Improper Resource Shutdown or Release
CVSS Source: emo@eclipse.org
CVSS Base score: 7.2
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)

CVEID: CVE-2025-1470
Description: In Eclipse OMR, from

from the initial contribution to version 0.4.0, some OMR internal port library and utilities consumers of z/OS atoe functions do not check their return values for NULL memory pointers or for memory allocation failures. This can lead to NULL pointer dereference crashes. Beginning in version 0.5.0, internal OMR consumers of atoe functions handle NULL return values and memory allocation failures correctly.
CWE: CWE-476: NULL Pointer Dereference
CVSS Source: NVD
CVSS Base score: 5.5
CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2025-1471
Description: In Eclipse OMR versions 0.2.0 to 0.4.0, some of the z/OS atoe print functions use a constant length buffer for string conversion. If the input format string and arguments are larger than the buffer size then buffer overflow occurs. Beginning in version 0.5.0, the conversion buffers are sized correctly and checked appropriately to prevent buffer overflows.
CWE: CWE-787: Out-of-bounds Write
CVSS Source: NVD
CVSS Base score: 7.8
CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-21587
Description: An unspecified vulnerability in Java SE related to the Server: DDL component could allow a remote attacker to cause high confidentiality and high integrity impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle.
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2025-30698
Description: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity and low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: Oracle.
CVSS Base score: 5.6
CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CVEID: CVE-2025-4447
Description: In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.
CWE: CWE-121: Stack-based Buffer Overflow
CVSS Source: NVD
CVSS Base score: 9.8
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-27152
Description: axios is a promise based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if baseURL is set, axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of axios. This issue is fixed in 1.8.2.
CWE: CWE-918: Server-Side Request Forgery (SSRF)
CVSS Source: IBM
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2025-27533
Description: Memory Allocation with Excessive Size Value vulnerability in Apache ActiveMQ. During unmarshalling of OpenWire commands the size value of buffers was not properly validated which could lead to excessive memory allocation and be exploited to cause a denial of service (DoS) by depleting process memory, thereby affecting applications and services that rely on the availability of the ActiveMQ broker when not using mutual TLS connections. This issue affects Apache ActiveMQ: from 6.0.0 before 6.1.6, from 5.18.0 before 5.18.7, from 5.17.0 before 5.17.7, before 5.16.8. ActiveMQ 5.19.0 is not affected. Users are recommended to upgrade to version 6.1.6+, 5.19.0+, 5.18.7+, 5.17.7, or 5.16.8 or which fixes the issue. Existing users may implement mutual TLS to mitigate the risk on affected brokers.
CWE: CWE-789: Memory Allocation with Excessive Size Value
CVSS Source: NVD
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/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 Secure Proxy	6.2.0.x
	6.1.0.x

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.1.0.0 - 6.1.0.1	6.1.0.2 GA / Fix Central
	6.2.0.0 - 6.2.0.1	6.2.0.2 GA / Fix Central

Workarounds and Mitigations
None.

Change History
28 Aug 2025: Initial Publication

IBM Sterling Secure Proxy is vulnerable to multiple issues.

Summary
Multple vulnerabilities affect IBM Sterling Secure Proxy and are addressed in the latest release and iFix

Vulnerability Details

CVEID: CVE-2024-30172
Description: The Bouncy Castle Crypto Package For Java is vulnerable to a denial of service, caused by an infinite loop in the Ed25519 verification code. By persuading a victim to use a specially crafted signature and public key, a remote attacker could exploit this vulnerability to cause a denial of service condition.
CWE: CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')
CVSS Source: IBM X-Force
CVSS Base score: 5.5
CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CVEID: CVE-2024-21094
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause no confidentiality impact, low integrity impact, and no availability impact.
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-21085
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low availability impacts.
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21011
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low availability impact.
CWE: CWE-770: Allocation of Resources Without Limits or Throttling
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2023-38264
Description: The IBM SDK, Java Technology Edition's Object Request Broker (ORB) 7.1.0.0 through 7.1.5.21 and 8.0.0.0 through 8.0.8.21 is vulnerable to a denial of service attack in some circumstances due to improper enforcement of the JEP 290 MaxRef and MaxDepth deserialization filters. IBM X-Force ID: 260578.
CWE: CWE-502: Deserialization of Untrusted Data
CVSS Source: IBM X-Force
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2024-21147
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality, high integrity impacts.
CWE: CWE-284: Improper Access Control
CVSS Source: IBM X-Force
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

CVEID: CVE-2024-21145
Description: An unspecified vulnerability in Java SE related to the 2D component could allow a remote attacker to cause low confidentiality, low integrity impacts.
CWE: CWE-284: Improper Access Control
CVSS Source: IBM X-Force
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21140
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality, low integrity impacts.
CWE: CWE-284: Improper Access Control
CVSS Source: IBM X-Force
CVSS Base score: 4.8
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVEID: CVE-2024-21144
Description: An unspecified vulnerability in Java SE related to the Concurrency component could allow a remote attacker to cause low availability impact.
CWE: CWE-284: Improper Access Control
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21138
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause a low availability impact.
CWE: CWE-770: Allocation of Resources Without Limits or Throttling
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CVEID: CVE-2024-21131
Description: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low integrity impact.
CWE: CWE-284: Improper Access Control
CVSS Source: IBM X-Force
CVSS Base score: 3.7
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-27267
Description: The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 7.1.5.18 and 8.0.0.0 through 8.0.8.26 is vulnerable to remote denial of service, caused by a race condition in the management of ORB listener threads. IBM X-Force ID: 284573.
CWE: CWE-300: Channel Accessible by Non-Endpoint
CVSS Source: IBM X-Force
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2024-22201
Description: Eclipse Jetty is vulnerable to a denial of service, caused by a flaw when an HTTP/2 connection gets TCP congested. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause the server to stop accepting new connections from valid clients, and results in a denial of service condition.
CWE: CWE-400: Uncontrolled Resource Consumption
CVSS Source: IBM X-Force
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CVEID: CVE-2024-41784
Description: IBM Sterling Secure Proxy could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot dot" sequences (/.../) to view arbitrary files on the system.
CWE: CWE-32: Path Traversal: '...' (Triple Dot)
CVSS Source: IBM X-Force
CVSS Base score: 7.5
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2021-40690
Description: Apache Santuario XML Security for Java could allow a remote attacker to bypass security restrictions, caused by the improper passing of the "secureValidation" property when creating a KeyInfo from a KeyInfoReference element. An attacker could exploit this vulnerability to abuse an XPath Transform to extract any local .xml files in a RetrievalMethod element.
CWE: CWE-287: Improper Authentication
CVSS Source: IBM X-Force
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

CVEID: CVE-2024-3933
Description: Eclipse Openj9 could allow a local authenticated attacker to bypass security restrictions, caused by the failure to restrict access to a buffer with an incorrect length value when executing an arraycopy sequence while the Concurrent Scavenge Garbage Collection cycle is active and the source and destination memory regions for arraycopy overlap. By sending a specially crafted request, an attacker could exploit this vulnerability to gain read and write to addresses beyond the end of the array range.
CWE: CWE-805: Buffer Access with Incorrect Length Value
CVSS Source: IBM X-Force
CVSS Base score: 5.3
CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:L)

CVEID: CVE-2023-29262
Description: IBM Sterling Secure Proxy is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.
CWE: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVSS Source: IBM X-Force
CVSS Base score: 5.4
CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.0.0.0 6.0.1.0 6.0.2.0 6.0.3.0 6.1.0.0

Following versions are affected by these CVEs (CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21138, CVE-2024-21131, CVE-2024-27267).

Affected Product(s)	Version(s)
IBM Sterling Secure Proxy	6.0.0.0 - 6.0.3.1
	6.1.0.0 - 6.1.0.1
	6.2.0.0 - 6.2.0.1

Remediation/Fixes

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.0.0.0 6.0.1.0 6.0.2.0 6.0.3.0	6.0.3.1 GA / Fix Central
	6.1.0.0	6.1.0.1 GA / Fix Central

These CVEs (CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21138, CVE-2024-21131, CVE-2024-27267) are fixed in below mentioned fix versions.

Product	Version	Fixed-in Version(s) / Remediation
IBM Sterling Secure Proxy	6.0.0.0 - 6.0.3.1	6.0.3.1 iFix 03 / Fix Central
	6.1.0.0 - 6.1.0.1	6.1.0.1 iFix 03 / Fix Central
	6.2.0.0 - 6.2.0.1	6.2.0.1 iFix 02 /Fix Central

Workarounds and Mitigations
None.

Change History
21 Oct 2024: Initial Publication.

Known issues in Sterling B2B Integrator

Last Updated: 2025-11-12

Before you use Sterling B2B Integrator, you must ensure to understand the known issues that might need you to follow certain workarounds for smooth functioning.

The following sections provide a list of Known Issues specific to every version.

- 6.2.1.x
- 6.2.1.1

List of known issues for v6.2.1.x

The following list of known issues apply to Sterling B2B Integrator v6.2.1.0 and later.

Functionality	Known Issue	Workaround
Installation of IBM® Sterling B2B Integrator using IBM Installation Manager (IIM)	When installing IBM Sterling B2B Integrator on RHEL 9.x OS based on x86-64 and Power 10 little endian hardware, GTK package versions greater than 3.22.30 cause some checkboxes and radio buttons to appear incorrectly. This is due to an IIM limitation.	Before launching IIM, ensure that the GTK package version in the OS is 3.22.30.
SAP Suite Adapter for JCo3x	When configured for adapter containers, SAP Suite Adapter for JCo3x remains disabled. **Note:** This issue is applicable only for certified container images.	No workaround.
Azure SQL Database	When Sterling B2B Integrator v6.2.1.0 and higher is installed with Azure SQL Database, running the **dump_info.cmd** script results in an error.	No workaround.
Upgrading IBM Sterling B2B Integrator from v5.2.6.3_x to v6.2.1.0.	Upgrading IBM Sterling B2B Integrator from v5.2.6.3_x (or lower) to v6.2.1.0 fails due to v5.2.6.3_x running on JDK 7.	1. Stop the Sterling B2B Integrator instance v5.2.6.3_x or lower. 2. Run the command: **upgradeJDK.sh <path to IBM JDK 8.0.6.20> <path to JCE policy File>** 3. Upgrade IIM to v1.10.1. Using the upgraded IIM, upgrade Sterling B2B Integrator to v6.2.1.0. This can be done using the GUI mode or by using a response file, while specifying IBM Semeru Runtime Certified Edition 17.0.14.0 (build 17.0.14+7).
Upgrading IBM Sterling B2B Integrator with NIST enabled.	Upgrading IBM Sterling B2B Integrator from v5.2.6.5_x to v6.2.1.0 fails. Upgrading IBM Sterling B2B Integrator from v6.0.0.8 to v6.2.1.0 fails.	1. Disable NIST by setting NIST_MODE=off in sandbox.cfg. 2. Run the command: **deployer.sh** or **deployer.cmd** 3. Perform the upgrade to v6.2.1.0. 4. Re-enable NIST by setting NIST_MODE=strict after completing the upgrade.

Functionality	Known Issue	Workaround
Upgrading IBM Sterling B2B Integrator on AIX	• IIM v1.10.1 and IBM Packaging Utility no longer support 32-bit architecture on AIX systems. Starting with release 1.10.1, IIM requires 64-bit Version 11 Java and does not provide GUI support for AIX. Users on a 32-bit platform must transition to a 64-bit platform to install or upgrade to version 1.10.1.	For users already on a 64-bit platform, the **reInstallIM** command can be used to transition IIM from a 32-bit to a 64-bit architecture: 1. To perform this upgrade, run the command: **./userinstc -reinstallIM -acceptLicense** Use the response file to install or upgrade Sterling B2B Integrator to v6.2.1.0.
ITXA Integration	In an IIM Sterling B2B Integrator and ITXA setup, SSO will not work in Sterling B2B Integrator v6.2.0.0-ITX 10.1.1.1-ITXA 10.0.1.7 setup and prior ITXA releases. Although SSO is not working, it will not affect the E2E runtime flows	To use the ITXA UI: Comment the following properties in customer.overrides.props to ensure ITXA is a run as a standalone environment: ○ SI-SPE Integration ○ HostApplication.name=SBI ○ HostApplication.migrationStylesheet=ie_si_to_spe_hosted ○ HostApplication.driverName=InvokeSIBP ○ HostApplication.driverClass=com.ibm.spe.core.drivers.DriverInvokeSIBusinessProcess ○ HostApplication.restURL=https://<hostname>:<base port+60>/restwar/restapi/v1.0 2. Restart the ITXA TPUI server. **Note:** To return to integration mode with Sterling B2B Integrator, uncomment the above properties and restart the ITXA TPUI server.
myFileGateway 2.0	While installing Sterling B2B Integrator using the IBM Installation Manager, if myFileGateway 2.0 is hosted on multiple HTTP Server Adapter on AC and ASI nodes, you must access the adapter configured in sandbox.cfg. The following properties contain the information of the configured adapters in sandbox.cfg: ASI_SERVICE_HOST = CHANGEME ASI_SERVICE_PORT = CHANGEME MYFG_PROTOCOL=http **Tip:** Value for **MYFG_PROTOCOL** can be **http** or **https**.	No workaround.
	While installing Sterling B2B Integrator using Certified Container, if myFileGateway 2.0 is hosted on multiple HTTP Server Adapter on AC and ASI nodes, then you must access the adapters configured in values.yaml. The following properties contain the information of the configured adapters	

Functionality	Known Issue	Workaround
	in values.yaml. myFgAccess: myFgPort: myFgProtocol:	
	Unable to login to myFileGateway 2.0 in zLinux.	IIM: 1. Update the JVM options in bin/tmp.sh. 2. Modify the *JAVA_FLAGS* variable as follows: JAVA_FLAGS="-Djava.io.tmpdir=/B2B/IBM/SI_6210/tmp -Djdk.tls.namedGroups="secp256r1,secp384r1"" 3. Restart the server. Login to myFileGateway 2.0.
		Certified Container: To resolve the issue with HTTPS access to dashboard when the parameter **useSslForRmi** is set to true and the myFileGateway 2.0 login issue: 1. Update the **jvmOptions** flag for ASI, AC, and API pods as follows: jvmOptions: -Djdk.tls.namedGroups=secp256r1,secp384r1 2. Perform a helm upgrade. Login to myFileGateway 2.0.
	While installing Sterling B2B Integrator using Certified Container, if myFileGateway 2.0 is hosted on multiple HTTP Server Adapter on AC and ASI nodes, then you must access the adapters configured in values.yaml. The following properties contain the information of the configured adapters in values.yaml. myFgAccess: myFgPort: myFgProtocol:	
Out-of-the-box (OOTB) Adapters	When upgrading from Sterling B2B Integrator v6.1.2.x IIM to 6.2.1.0 container deployment, the OOTB adapter ports do not update according to the base port values specified in values.yaml.	Manually update the REST HTTP Server Adapter port with the value: base port + 60.
SWIFTNet7 Adapter	SWIFTNet7 adapter fails to restart if the connection is lost on AIX MEFG deployment. This issue persists only on SWIFTNet 7.7.	Manually restart the SWIFTNet7 adapter to recover from a connection loss.
FIPS 140-3	FIPS 140-3 Strict mode is unsupported.	No workaround.
Hardware Security Module (HSM)	The keys created on the nCipher HSM device using earlier Sterling B2B Integrator versions with the IBM PKCS11 provider do not work in version 6.2.1.0.	No workaround.

Functionality	Known Issue	Workaround
Sterling B2B Integrator API Server	API Server fails to load. This issue occurs when the property **noapp.retain.libertyProps.customization** is set to true in customer_overrides.properties, and Sterling B2B Integrator is upgraded to v6.2.1.0. This issue does not occur if the property is not set or set to false.	Set **noapp.retain.libertyProps.customization=false** in customer_overrides.properties before performing the upgrade. **Note:** • This setting will reset the configurations in server.xml to the default values. Any customizations made to the server.xml must be manually re-applied after the upgrade. Features that are unsupported in Jakarta EE Web Profile 10.0 will fail. For more information, see Jakarta EE Web Profile 10.0 documentation.
ITX/ITXA Integration	ITX/ITXA Integration is unsupported in this release.	No workaround.
Business Process as a Service (BPaaS)	Business process fails with the following error: Processing error has occurred. Please contact the system administrator and check logs for more details: java.lang.IllegalStateException: This key is no longer valid	To resolve this issue, update Sterling B2B Integrator Liberty server's JVM options to include the required JAR file, then restart the server: 1. Stop Sterling B2B Integrator Liberty server. Use either of the following methods: ○ Run: kill -9 <SILibertyPID> ○ Run: hardstop.sh 2. Update JVM options by navigating to <SI_InstallDir>/liberty/wlp/usr/servers/SIServer and add the following line to *jvm.options*: -Xbootclasspath/a:/liberty/wlp/usr/servers/SIServer/apps/APIjarsLib/bcprov-jdk18on-1.78.1.jar 3. Restart Sterling B2B Integrator Liberty server. Use either of the following scripts: ○ startLiberty.sh ○ run.sh
ASI Pod	ASI pod keeps restarting on zlinux.	To resolve the issue, perform the following steps: 1. Update the **jvmOptions** flag for ASI, AC, and API pods as follows: jvmOptions: -Djdk.tls.namedGroups=secp256r1,secp384r1 Perform a helm upgrade.

List of known issues for v6.2.1.1

The following list of known issues apply to Sterling B2B Integrator v6.2.1.1:

Functionality	Known Issue	Workaround
Certified Containers - Adapters and Business Processes (BPs)	When you edit adapters or BPs in a certified containers environment, the process may occasionally become unresponsive or freeze.	To fix this issue, perform the following steps: 1. Copy the file centralops.properties.in outside the pod or to the resources mount location. Use the following command: kubectl/oc cp <namespace>/<asi-pod>:/ibm/b2bi/install/properties/centralops.properties.in <dir location>/centralops.properties.in **Note:** Replace <dir location>with the desired destination path. 2. Update the property **libertyJndi=false** in the copied file. 3. Put the updated file in the <helm-charts>/config folder directory. Perform a Helm upgrade.

Known Issues

Last Updated: 2025-11-12

This topic lists the known issues in Global Mailbox. Before you use Global Mailbox, you must ensure to understand the known issues that might need you to follow certain workarounds for smooth functioning.

Functionality	Known Issue	Workaround
Installation	Starting all Global Mailbox servers simultaneously during initial setup can lead to replication failures.	Global Mailbox servers must be started one at a time during initial setup.
Upgrade	After upgrading Sterling B2B Integrator or Global Mailbox from v6.1.0.x to 6.2.1.x, the configurations for securing Cassandra JMX will be lost.	You must reconfigure Cassandra to secure the JMX connections. For more information, see Securing Cassandra JMX.
Initial setup	There are port conflict errors or security concerns observed for the port number 9160. It is the port number used by Thrift RPC server in Cassandra.	Cassandra doesn't use the Thrift RPC server any longer. If you face security concerns or any other issue on the port number 9160, you can edit the **cassandra.yaml** from the location <cassandra install location>/conf and set **start_rtc:false**.
Initial setup	When trying to start admin servers at the same time during the initial setup, a 1970 date is written into the replication_queue_ptr table in the database and files are not replicated.	Start Global Mailbox Admin servers one at a time during the initial setup (while the replication_read_ptr table is empty or after it has been truncated). After the initial setup, you can start Global Mailbox Admin servers at the same time.
Administrator user interface	The administrator UI for Global Mailbox cannot be reached from the Sterling B2B Integrator administrator UI when all replication servers in a data center are manually suspended. Error dialogs indicate the Global Mailbox client adapter cannot be found.	Administrative activity for Global Mailbox must be performed by directly accessing the Global Mailbox administrative UI.
ASCP	ASCP frequently generates logs about session shutdown failures.	Ignore **Session shutdown failure** errors. This is a normal condition.
Standby queue manager	The Event Rule Adapter configuration shows an empty value for the Connection Name list rather than listing the active and standby queue managers.	Configure the Global Mailbox Event Rule Adapters in Sterling B2B Integrator to use a connection list with both the active and standby queue managers in the list. You should only list queue managers in the same datacenter as the Sterling B2B Integrator node that you are configuring.
Performance	Due to limitations in the Cassandra Repair jobs, Global Mailbox can process 500,000 messages per day.	If your production environment must support a higher load of messages per day, contact IBM Support.
	The highest measured peak throughput with Global Mailbox is 70 messages per second.	If your production environment must support a higher load of messages per day, contact IBM Support.
	Each Global Mailbox server consumes 1 CPU core while idle.	Allocate sufficient CPU resources to all servers.
Non-English topics	Information about firewall configuration was not translated.	Ensure that your firewalls are configured to allow connections to the ports for ZooKeeper, Cassandra, Global Mailbox Management, MQ, and Sterling B2B Integrator nodes.

Functionality	Known Issue	Workaround
Non-English topics	Updated information about recovering from a planned or unplanned data center outage was not translated.	Use the English version of the topics *Restarting Cassandra nodes after data center maintenance* and *Restarting the Global Mailbox management node*.
Non-English topics	Updated information for configuring advanced event processing was not translated.	Use the English version of the topic *Configuring IBM MQ advanced event management*.
Upgrading Global Mailbox on AIX	• IIM v1.10.1 and IBM Packaging Utility no longer support 32-bit architecture on AIX systems. Starting with release 1.10.1, IIM requires 64-bit Version 11 Java and does not provide GUI support for AIX. Users on a 32-bit platform must transition to a 64-bit platform to install or upgrade to version 1.10.1.	For users already on a 64-bit platform, the **reInstallIM** command can be used to transition IIM from a 32-bit to a 64-bit architecture: 1. To perform this upgrade, run the command: **./userinstc -reinstallIM -acceptLicense** Use the response file to install or upgrade Sterling B2B Integrator to v6.2.1.0.

Important Reminder B2Bi / SFG v6.1.x End of Support

Abstract
End of support of IBM Sterling B2B Integrator (B2Bi) version 6.1.x is April 30, 2026.

Content
End of support of IBM Sterling B2B Integrator (B2Bi) version 6.1.x is April, 30 2026.

This includes all releases in the 6.1.x streams including:

B2Bi & SFG Versions

6.1.0.0, 6.1.0.1, 6.1.0.2, 6.1.0.3, 6.1.0.4, 6.1.0.4_1, 6.1.0.4_1A, 6.1.0.4_2, 6.1.0.5, 6.1.0.5_1, 6.1.0.5_2, 6.1.0.6, 6.1.0.7, 6.1.0.8, ...

6.1.1.0, 6.1.1.0_1, 6.1.1.0_1A, 6.1.1.0_2, 6.1.1.1, 6.1.1.2, 6.1.1.3, 6.1.1.4

6.1.2.0, 6.1.2.1, 6.1.2.2, 6.1.2.3, 6.1.2.4, 6.1.2.5, 6.1.2.5_1, ...

For more information, see Product Lifecycle page: https://www.ibm.com/support/pages/node/6334789

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