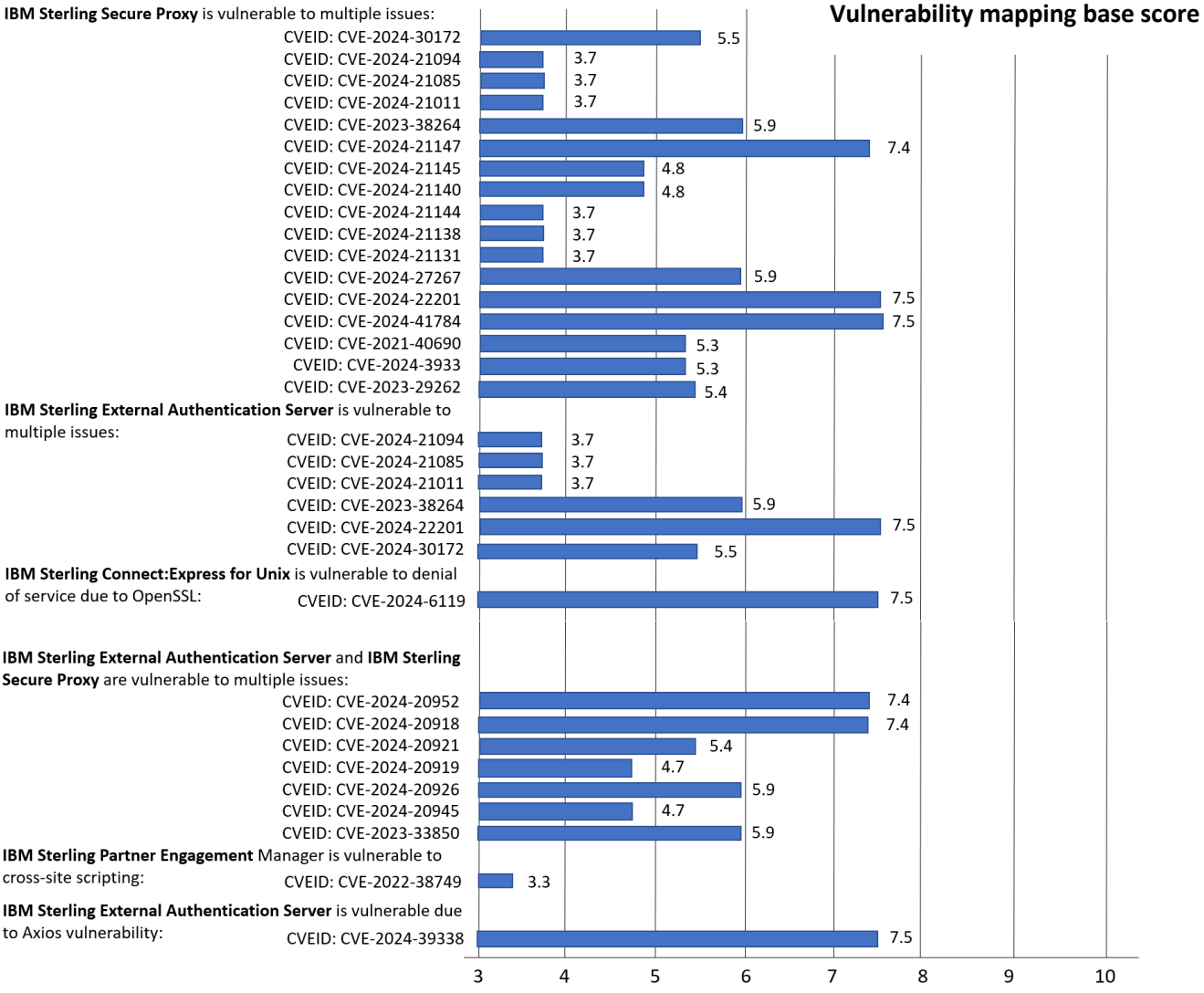
B2B Solutions
Let's build IT together

Integration News

T3 2024

In this issue:

IBM Sterling B2B Data Exchange Solutions. SECURITY NEWS:



Other contents:

- What's new in **IBM Sterling B2B Integrator 6.2.0.3**
- Important Reminder **B2Bi / SFG v6.1.x** End of Support
- **IBM Sterling B2B Integrator** Clustering Architecture
- **IBM Sterling B2B Integrator** Network Flow Graph
- **IBM Sterling Connect:Direct for UNIX** Upgrade Considerations. Question & Answer

IBM Sterling Secure Proxy is vulnerable to multiple issues.

Summary

Multiple 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
IBM Sterling Secure Proxy	6.1.0.0

Remediation/Fixes

Product	Affected 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
IBM Sterling Secure Proxy	6.1.0.0	6.1.0.1 GA	Fix Central

Workarounds and Mitigations
None Known.

Change History:
21 Oct 2024: Initial Publication23 Oct 2024: Updated Version(s)
*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

IBM Sterling External Authentication Server is vulnerable to multiple issues.

Summary

Multiple vulnerabilities affect IBM Sterling External Authentication Server and are addressed in the latest iFixes.

Vulnerability Details

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-2024-22201

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-2024-30172

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)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Secure External Authentication Server	6.0.0.0 6.0.1.0 6.0.2.0 6.0.3.0
IBM Sterling External Authentication Server	6.1.0.0 6.1.0.1

Remediation/Fixes

Product	Affected Version	Fixed-in Version(s)	Remediation
IBM Sterling External Authentication Server	6.0.0.0 6.0.1.0 6.0.2.0 6.0.3.0	6.0.3.1 GA	Fix Central
IBM Sterling External Authentication Server	6.1.0.0 6.1.0.1	6.1.0.2 GA	Fix Central

Workarounds and Mitigations
None Known.

Change History
21 Oct 2024: Initial Publication23 Oct 2024: Updated Affected / Fixed Version

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

IBM Sterling Connect:Express for UNIX is vulnerable to denial of service due to OpenSSL

Summary

OpenSSL is used by IBM Sterling Connect:Express for UNIX. IBM Sterling Connect:Express for UNIX has addressed the applicable CVE.

Vulnerability Details

CVEID: CVE-2024-6119

DESCRIPTION: OpenSSL is vulnerable to a denial of service, caused by an error when performing certificate name checks (e.g., TLS clients checking server certificates). By sending a specially crafted request, a remote attacker could exploit this vulnerability to read an invalid memory address resulting in abnormal termination of the application process.

CWE: CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')
CVSS Source: CISA ADP
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)
Sterling Connect:Express for UNIX	1.5.x

Remediation/Fixes

Product	Version	Remediation/ Fix/ Instructions)
IBM Sterling Connect: Express for UNIX	1.5.0.1700 and prior	Upgrade to 1.5.0.17010 or apply the OpenSSL 3.3.2 Updater for Connect:Express for Unix. Both are available on Fix Central.

Workarounds and Mitigations
None.

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 iFixes.

Vulnerability Details

CVEID: CVE-2024-20952
DESCRIPTION: An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause high confidentiality impact and high integrity impact.
CWE: CWE-416: Use After Free
CVSS Source: CVE.org
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-2024-20918
DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact and high integrity impact.
CWE: CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
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-2024-20921
DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high confidentiality impact.
CWE: CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
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)

CVEID: CVE-2024-20919
DESCRIPTION: An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause high integrity impact.

CVSS Source: IBM X-Force
CVSS Base score: 4.7
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2024-20926

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

CWE: CWE-20: Improper Input Validation
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)

CVEID: CVE-2024-20945

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

CWE: CWE-20: Improper Input Validation
CVSS Source: IBM X-Force
CVSS Base score: 4.7
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2023-33850
DESCRIPTION: IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information.
CWE: CWE-203: Observable Discrepancy
CVSS Source: IBM
CVSS Base score: 5.9
CVSS Vector:
(CVSS:3.1/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 Secure External Authentication Server	6.0.3
IBM Secure External Authentication Server	6.1.0

Remediation/Fixes

Product	Version	Fixed-in Version(s)/ Remediation /Fix
IBM Secure External Authentication Server	6.0.0.0 6.0.1.0 6.0.2.0 6.0.3.0	6.0.3.1 GA Fix Central
IBM Secure External Authentication Server	6.1.0.0 6.1.0.1	6.1.0.2 GA Fix Central

Workarounds and Mitigations
None.

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-2024-20952

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

CWE: CWE-416: Use After Free
CVSS Source: CVE.org
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-2024-20918

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

CWE: CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
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-2024-20921

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

CWE: CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
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)

CVEID: CVE-2024-20919

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

CWE: CWE-20: Improper Input Validation
CVSS Source: IBM X-Force
CVSS Base score: 4.7
CVSS Vector:
(CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)

CVEID: CVE-2024-20926

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

CWE: CWE-20: Improper Input Validation
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)

CVEID: CVE-2024-20945

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

CWE: CWE-20: Improper Input Validation
CVSS Source: IBM X-Force
CVSS Base score: 4.7
CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CVEID: CVE-2023-33850

DESCRIPTION: IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information.

CWE: CWE-203: Observable Discrepancy
CVSS Source: IBM
CVSS Base score: 5.9
CVSS Vector: (CVSS:3.1/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 6.0.1.0 6.0.2.0 6.0.3.0
IBM Sterling Secure Proxy	6.1.0.0

Remediation/Fixes

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

Workarounds and Mitigations
None.

IBM Sterling Partner Engagement Manager is vulnerable to cross-site scripting

Summary

IBM Sterling Partner Engagement Manager has addressed a reflected cross-site scripting vulnerability.

Vulnerability Details

CVEID: CVE-2022-38749

DESCRIPTION: SnakeYAML is vulnerable to a denial of service, caused by a stack-overflow in parsing YAML files. By persuading a victim to open a specially crafted file, a remote attacker could exploit this vulnerability to cause the application to crash.

CWE: CWE-787: Out-of-bounds Write
CVSS Source: IBM X-Force
CVSS Base score: 3.3
CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L)

Affected Products and Versions

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

Remediation/Fixes

Product	Version	Fixed-in Version(s)/ Remediation/Fix
IBM Sterling Partner Engagement Manager Essentials Edition	6.1.*, 6.2.*	Download 6.1.2.10 Download 6.2.3.2
IBM Sterling Partner Engagement Manager Standard Edition	6.1.*, 6.2.*	Download 6.1.2.10 Download 6.2.3.2

Workarounds and Mitigations
None.

IBM Sterling External Authentication Server is vulnerable due to Axios vulnerability

Summary

IBM Sterling External Authentication Server (SEAS) uses Axios, which is vulnerable to Server-side Request Forgery (SSRF).

Vulnerability Details

CVEID: CVE-2024-39338

DESCRIPTION: Axios is vulnerable to server-side request forgery, caused by a flaw with requests for path relative URLs get processed as protocol relative URLs. By sending a specially crafted request, an attacker could exploit this vulnerability to conduct SSRF attack.

CWE: CWE-918: Server-Side Request Forgery (SSRF)
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:H/I:N/A:N)

Affected Products and Versions

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

Remediation/Fixes

Product	Affected Version	Fixed-in Version(s)	Remediation
IBM Sterling External Authentication Server	6.1.0.0 - 6.1.0.2	6.1.0.2 ifix 01	Fix Central
IBM Sterling External Authentication Server	6.1.0.0 6.1.0.1	6.1.0.2 GA	Fix Central

Workarounds and Mitigations

None.

What's new in IBM Sterling B2B Integrator 6.2.0.3

New features

Following new features are introduced in this release:

- TLS 1.3 can now be configured for:
  - Command Line Adapter 2 (CLA2). For more information, see Command Line Adapter 2.
  - Lightweight Directory Access Protocol (LDAP). For more information, see Configure LDAP with Sterling B2B Integrator.
  - JMS 1.1 Async Receive Adapter. For more information, see JMS 1.1 Async Receive Adapter
  - Sterling Connect:Direct Requester Adapter. For more information, see Connect:Direct Requester Adapter.
  - Sterling Connect:Direct Server Adapter. For more information, see Connect:Direct Server Adapter.
  - SWIFTNet7 Adapter. For more information, see SWIFTNet7 Adapter.
  - WebSphere MQ Suite Open Session Service. For more information, see WebSphere MQ Suite Open Session Service and WebSphere MQ Suite - Security Considerations.
- Added support for **KEY_NEW_PATH** in SFTP 2.0 PUT After user exit.
- Certified Container enhancements:
  - Support for **subPath** configuration for extraPVCs in helm charts. For more information, see Sample values.yaml file for v6.2.0.3.
  - Support for enabling both logs volume and logging to console at the same time using the parameter **appLogsPVC.enabled**. For more information, see Configuring the Certified Container.

Important: Installing or upgrading IBM® Sterling B2B Integrator to v6.2.0.3 from any IBM Sterling B2B Integrator version is not supported when Federal Information Processing Standards (FIPS) mode is enabled. For more information, see IBM Sterling B2B Integrator and IBM Sterling File Gateway migration and upgrade paths for FIPS 140-2 end of support.

Stack updates

Note: This Fix pack also includes security fixes and stack upgrades from release 6202.

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

- Bouncy Castle - 1.78.1
- CKEditor - 4.24
- Java - 8.0.8.25
- Meig jars - 1.0.0.10_1
- MQ client jars - 9.3.0.20
- Spring framework - 5.3.34
- Websphere Liberty - 24.0.0.7

For more information, see Software Product Compatibility Report.

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

End of support of IBM Sterling B2B Integrator (B2Bi) version 6.1.x is September, 30 2025.

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.

URGENT NOTE: If you are on a custom specific interimFix (sometimes called “hotfix”) please check either yourself or via Support if all the fixes from your custom interimFix are incorporated to the core product version of B2Bi/SFG.

For information on the latest release, see SB2BI V6.2 Document.

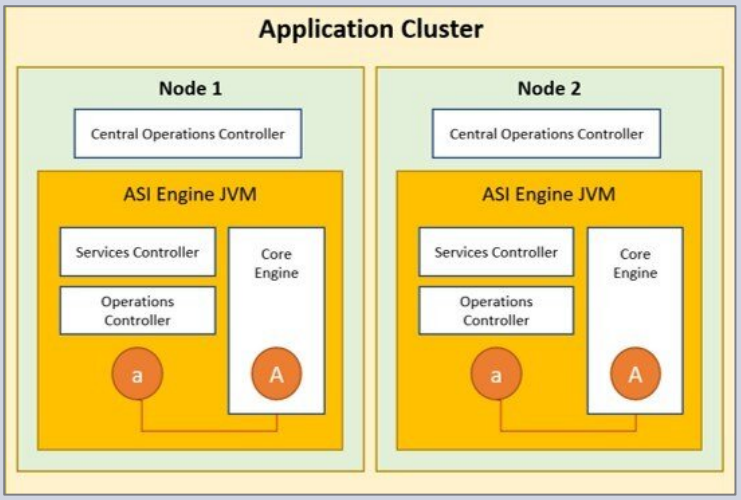
IBM Sterling B2B Integrator Clustering Architecture

Clustered installations of Sterling B2B Integrator use the different components of a node (that is, one of the cluster installations).

These include:

- Core engine components, which execute business processes.
- Services and adapters, which execute business process steps and communicate with external systems such as databases, ERP (enterprise resource planning) and CRM (customer relationship management) systems, and other technologies and packages.
- The Operations Controller, which manages resources across Java™ Virtual Machine (JVM) boundaries.
- The Services Controller, which provides the mechanisms to manage, configure, query, and cache all service/adapter-related information.
- The Central Operations Controller, which provides a single point of contact for all operational questions and communicates with the Operations Controller to coordinate component operations.

The following diagram illustrates a basic cluster configuration. “ASI” stands for Application Server Independent. The instances of lowercase and uppercase letter “A” refer to different parts of adapters.



- **Resource Sharing in a Clustered Installation**
  ASI clustering locates resources throughout the cluster using the Java Naming Directory Interface (JNDI), which is a standard technology that enables configuration information to be shared locally and across a network.
- **ASI Engine and Workflow Queuing in a Clustered Installation**
  In a cluster, performance is affected by the number of threads allocated for each queue on each cluster node. Load balancing is dependent on the number of threads and the number of steps for a business process to execute before being rescheduled and then possibly distributed to another node.
- **Load Balancing in a Clustered Installation**
  Clusters distribute business processes internally using a load-balancing algorithm determined by the scheduling policy. In addition, external load balancing mechanisms distribute incoming HTTP, FTP or other network traffic.
- **Multicast Workload Communications in a Clustered Installation**
  Multicast is used by an ASI cluster node to make information about its workload available to the rest of the cluster.
- **JGroups Workload Communications in a Clustered Installation**
  Communication among cluster nodes about the workload of each node helps provide business process load balancing. You have a choice between multicast communication (which services all requests with a single stream of data) and unicast communication (which services each request with its own stream of data).
- **About Operations Controllers in a Clustered Installation**
  Each application server component has an operations controller, which provides local and remote interfaces for controlling a server component and inquiring about its status.
- **Specifying Mandatory or Preferred Nodes for BP Steps in a Clustered Installation**
  Each service step in a business process can be configured to be executed on a particular node. This feature keeps business process steps local to a non-clusterable adapter and moves a business process to the correct node to access a document stored on disk.

- **Specifying Nodes as Execution Roles for BPs in a Clustered Installation**
  When a business process is configured to run on an execution role, the business process will be executed only on nodes assigned to do the specific execution role.
- **Business Process Recovery in a Clustered Installation**
  When a cluster node fails, Sterling B2B Integrator reacts like it would when a single node environment goes down in a non-clustered implementation.
- **Document Storage in a Clustered Installation**
  Sterling B2B Integrator provides the option of using document storage either in a local file system or a database. In cluster mode, the default for document storage is the database since all nodes use the same database, and a business process running on any node has access to the document for processing.

IBM Sterling B2B Integrator Network Flow Graph

In the OpenShift container environments there are multiple ways to configure the networking stack and depending on the configuration some of the resources like **NetworkPolicies** can be enforced differently.

Important: Sterling B2B Integrator limits the number of exposed ports and clearly documents them for client network management. Exposing more ports than necessary or not clearly documenting these ports runs the risk of crossing a client's network security team.

A network administrators can refer the following network map to properly secure their cluster and the workloads on the cluster:

Note: Below network map is based on the default out of the box port configurations only.

From	To	Port	Property	Protocol	Function
Ingress controller	ASI pod	50000	setupCfg.basePort	HTTP	Standard communication from Ingress controller to ASI Pod
Ingress controller	ASI front end service - HTTP	35000	asi.frontendService.ports.http	HTTP	Standard communication from Ingress controller to ASI front end service
Ingress controller	ASI front end service - HTTPs	35001	asi.frontendService.ports.https	HTTPS	Standard communication from Ingress controller to ASI front end service
Ingress controller	ASI front end service - websevices	35002	asi.frontendService.ports.soa	HTTP	Standard communication from Ingress controller to ASI front end service
Ingress controller	ASI front end service – ssl websevices	35003	asi.frontendService.ports.soassl	HTTPS	Standard communication from Ingress controller to ASI front end service
Ingress controller	ASI front end service – REST HTTP	35007	asi.frontendService.ports. restHttpAdapter	HTTP	Standard communication from Ingress controller to ASI front end service
Ingress controller	AC (Adapter Container) front end service - HTTP	35004	ac.frontendService.ports.http	HTTP	Standard communication from Ingress controller to AC front end service
Ingress controller	Liberty front end service - HTTP	35005	api.frontendService.ports.http	HTTP	Standard communication from Ingress controller to API front end service
Ingress controller	Liberty front end service - HTTPs	35006	api.frontendService.ports.https	HTTPs	Standard communication from Ingress controller to API front end service
Ingress controller	ITXA web services	443	itxaIntegration.sso	HTTPS	Standard communication from Ingress controller to ITXA web services

Sterling Connect:Direct for UNIX Upgrade Considerations. Question & Answer

Question

What are the upgrade considerations for Connect:Direct for UNIX v6.3.x/v6.4.x?

Cause

Upgrading from Connect:Direct for UNIX v6.0.x/v6.1.x/v6.2.x to Connect:Direct for UNIX v6.3.x/v6.4.x.

Answer

ATTENTION: Customers using Connect:Direct for UNIX v4.2.x! This product reached END OF SUPPORT on September 30 2021. IBM® Support no longer supports this product.

ATTENTION: Customers using Connect:Direct for UNIX v4.3.x! This product reached END OF SUPPORT on April 30 2023. IBM® Support no longer supports this product.

ATTENTION: Customers using Connect:Direct for UNIX v6.0.x! This product reached END OF SUPPORT on April 30 2024. IBM® Support no longer supports this product.

ATTENTION: Customers using Connect:Direct for UNIX v6.1.x! This product will reach END OF SUPPORT on April 30 2025. IBM® Support will no longer support this product after this date.

ATTENTION: Customers using Connect:Direct for UNIX v6.2.x! This product will reach END OF SUPPORT on September 30 2025. IBM® Support will no longer support this product after this date.

See the following announcement:
https://www.ibm.com/support/pages/lifecycle/search?q=connect%3Adirect%20for%20unix

PLAN YOUR UPGRADES ACCORDINGLY!

Note: CDU v6.3.x/v6.4.x versions are 64-bit applications.

Note: CDU v6.3.x/v6.4.x contains the Integrated File Agent. Connect:Direct Web Services is required to configure this version of File Agent. See the online CDU v6.3.x/v6.4.x System Guide for details. If desired, the Standalone File Agent will also work with CDU v6.3.x/v6.4.x.

Note: Starting with CDU v6.3.0.3, IBM Semeru Java JRE 17 is now used. The Secure+ Keystore is now PKCS12 format. IBM Key Manager is no longer provided. The upgrade process will automatically convert the old CMS format Keystore to the new PKCS12 format Keystore. You can use Keytool to manage certificates. Reference this Technote.

https://www.ibm.com/support/pages/node/7172585

Note: To upgrade to CDU v6.3.x, the base version of CDU must be at least version 6.0.x. If you have an older version than CDU v6.0.x, you must first upgrade successfully to at least CDU v6.0.x; and then upgrade to CDU v6.3.x.

Note: To upgrade to CDU v6.4.x, the base version of CDU must be at least version 6.1.x. If you have an older version than CDU v6.1.x, you must first upgrade successfully to at least CDU v6.1.x and then upgrade to CDU v6.4.x.

Things to do before upgrading:

1. Take a snapshot of your current UNIX server hosting the CDU installation for safe keeping.
2. During the upgrade, there is an option presented to backup the original installation, make sure you choose to do this. If you need to revert back to the original installation, you can run the installer again and you will be given the option to restore the previous version. You will need the password for 'root' to complete the backup process.
3. Make sure you always use the installer from the new CDU version. Do not use the installer from previous versions.
4. From the '/ndm/bin' folder, run 'cfgcheck'. This will verify the initparm, netmap, userfile, and ndmapi configuration files for correctness. You will need to correct any errors presented before proceeding with the upgrade. Errors in the configuration files can cause the upgrade to fail.
5. Using either the Secure+ Admin tool or the Secure+ CLI, do the following two functions.
    a) The Parmfile. Before attempting the upgrade from CDU v6.0.x/v6.1.x/v6.2.x to CDU v6.3.x/v6.4.x, you need to ensure that the node records in the Secure+ parmfile are in the correct v6.0.x/v6.1.x/v6.2.x format. To do this, you need to rekey the parmfile. Any node records not in the correct v6.0.x/v6.1.x/v6.2.x format will be set correctly.
        - From Secure+ Admin tool, click on 'File - Rekey Secure+'.
        - From Secure+ CLI, enter the command: 'rekey parmfile passphrase=<32-character alphanumeric string>;'. You will enter a 32-character alphanumeric passphrase. You do not need to remember this passphrase.

b) Validate the Parmfile. This will confirm that the Secure+ configuration is in order. If any errors are presented, you will need to correct these errors before doing the upgrade. Warnings are acceptable - but correct the errors. Errors could include invalid or expired certificates. Secure+ errors can cause the upgrade to fail.
    - From Secure+ Admin tool, click on 'File - Validate Secure+'.
    - From Secure+ CLI, enter the command: 'validate parmfile;'.

6. It is advisable that you practice the upgrade process in a test environment before going into production.
7. To do the upgrade, logon on to the UNIX system with the user ID that owns the current CDU installation. Do not use 'root'. You will need the password for 'root' to do the upgrade. Make sure you have access to the password for 'root'.
8. You should use the current maintenance package from IBM Support Fix Central for the CDU version being used to do the upgrade. The current maintenance packages are available from IBM Support Fix Central and can be used to do an upgrade from CDU v6.0.x/v6.1.x/v6.2.x. The upgrade instructions are given in the "Maintenance Installation Instructions" document that accompanies the Fixpack. You should always use the most current maintenance package available to do the upgrade. This will ensure that you have all current defect and security vulnerability patches in place.
9. Following are documents you need to read to perform a successful upgrade.
    a) Online CDU documentation. Pay special attention to the "Release Notes" and "Getting Started" sections. Please read the “Release Notes” for the current hardware and software requirements. Ensure that your UNIX OS is a supported version. v6.3.x v6.4.x
    b) Online documentation for installing v6.3.x and v6.4.x for use with AWS and other Object Store providers. v6.3.x v6.4.x
    c) Online documentation section covering Secure+. v6.3.x v6.4.x
    d) Online documentation section covering Integrated File Agent. v6.3.x v6.4.x
10. If you are using the Standalone Connect:Direct File Agent, you are are strongly encouraged to upgrade to the current maintenance package at this time. This is available from IBM® Fix Central. v1.4.0.3

Online PDF documentation for File Agent.

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