Security Bulletin: Multiple Vulnerabilities affect IBM Tivoli Netcool Impact

Security Bulletin

Summary

Multiple vulnerabilities were addressed in IBM Tivoli Netcool Impact version 7.1.0.38

Vulnerability Details

CVEID: CVE-2026-29063 *(https://www.cve.org/CVERecord?id=CVE-2026-29063)*
DESCRIPTION: Immutable.js provides many Persistent Immutable data structures. Prior to versions 3.8.3, 4.3.7, and 5.1.5, Prototype Pollution is possible in immutable via the mergeDeep(), mergeDeepWith(), merge(), Map.toJS(), and Map.toObject() APIs. This issue has been patched in versions 3.8.3, 4.3.7, and 5.1.5.
CWE: CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') *(https://cwe.mitre.org/data/definitions/1321.html)*
CVSS Source: security-advisories@github.com
CVSS Base score: 8.7
CVSS Vector: (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N)

CVEID: CVE-2025-7962 *(https://www.cve.org/CVERecord?id=CVE-2025-7962)*
DESCRIPTION: In Jakarta Mail 2.0.2 it is possible to preform a SMTP Injection by utilizing the \r and \n UTF-8 characters to separate different messages.
CWE: CWE-147: Improper Neutralization of Input Terminators *(https://cwe.mitre.org/data/definitions/147.html)*
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:H/A:N)

CVEID: CVE-2026-21945 *(https://www.cve.org/CVERecord?id=CVE-2026-21945)*
DESCRIPTION: Java SE is vulnerable to a denial of service, caused by an easily exploitable vulnerability issue that allows an remote attacker to cause a hang or repeatable crash of the application.
CWE: CWE-400: Uncontrolled Resource Consumption *(https://cwe.mitre.org/data/definitions/400.html)*
CVSS Source: secalert_us@oracle.com
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-2026-21932 *(https://www.cve.org/CVERecord?id=CVE-2026-21932)*
DESCRIPTION: Java SE could allow a remote attacker to bypass security controls and create, delete, or modify critical data or all accessible data, caused by an easily exploitable vulnerability.

CVSS Source: secalert_us@oracle.com
CVSS Base score: 7.4
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N)

CVEID: CVE-2026-21933 *(https://www.cve.org/CVERecord?id=CVE-2026-21933)*
DESCRIPTION: Java SE could allow a remote attacker to bypass security controls and perform unauthorized update, insert, delete, or read operations on accessible data, caused by an easily exploitable vulnerability.
CVSS Source: secalert_us@oracle.com
CVSS Base score: 6.1
CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CVEID: CVE-2026-21925 *(https://www.cve.org/CVERecord?id=CVE-2026-21925)*
DESCRIPTION: Java SE could allow a remote unauthenticated attacker to bypass security controls and perform unauthorized update, insert, delete, or read operations on accessible data, caused by an difficult to exploit vulnerability.
CVSS Source: secalert_us@oracle.com
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-2026-1188 *(https://www.cve.org/CVERecord?id=CVE-2026-1188)*
DESCRIPTION: In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. This issue is fixed in Eclipse OMR version 0.8.0.
CWE: CWE-131: Incorrect Calculation of Buffer Size *(https://cwe.mitre.org/data/definitions/131.html)*
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-2026-4788 *(https://www.cve.org/CVERecord?id=CVE-2026-4788)*
DESCRIPTION: IBM Tivoli Netcool Impact stores sensitive information in log files that could be read by a local user.
CWE: CWE-532: Insertion of Sensitive Information into Log File *(https://cwe.mitre.org/data/definitions/532.html)*
CVSS Source: IBM
CVSS Base score: 8.4
CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVEID: CVE-2025-53057 *(https://www.cve.org/CVERecord?id=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 *(https://cwe.mitre.org/data/definitions/284.html)*

CVSS Source: secalert_us@oracle.com

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 *(https://www.cve.org/CVERecord?id=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 *(https://cwe.mitre.org/data/definitions/200.html)*

CVSS Source: secalert_us@oracle.com

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-2020-36732 *(https://www.cve.org/CVERecord?id=CVE-2020-36732)*

DESCRIPTION: The crypto-js package before 3.2.1 for Node.js generates random numbers by concatenating the string "0." with an integer, which makes the output more predictable than necessary.

CWE: CWE-330: Use of Insufficiently Random Values *(https://cwe.mitre.org/data/definitions/330.html)*

CVSS Source: NVD

CVSS Base score: 5.3

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM Tivoli Netcool Impact	7.1.0.0 - 7.1.0.37

Remediation/Fixes

IBM strongly recommends addressing the vulnerability now by upgrading to 7.1.0 FP38

Product	VRMF	Remediation
IBM Tivoli Netcool Impact	7.1.0.38	Upgrade to IBM Tivoli Netcool Impact 7.1.0 Fix Pack 38 *(https://www.ibm.com/support/pages/node/7184732)* or later.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

Subscribe to My Notifications *(https://www.ibm.com/support/pages/node/718119)* to be notified of important product support alerts like this.

References

Complete CVSS v3 Guide

On-line Calculator v3

Related Information

IBM Secure Engineering Web Portal *(http://www.ibm.com/security/secure-engineering/bulletins.html)*

IBM Product Security Incident Response Blog *(http://www.ibm.com/blogs/psirt)*

Acknowledgement

Change History

01 Apr 2026: Initial Publication

*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.

Disclaimer

Document Information

More support for:

Tivoli Netcool/Impact *(https://www.ibm.com/mysupport/s/topic/0TO500000002JCzGAM)*

Software version:

7.1.0

Operating system(s):

AIX, Solaris, Linux, Linux on IBM Z Systems, Windows

Document number:

7268267

Modified date:

01 April 2026

Initial Publish date:

01 April 2026