Security Bulletin: IBM TX Standard is affected by an Out-of-bounds Write vulnerability and by a Use of Inherently Dangerous Function vulnerability due to the way that the product uses certain C library functions.

Security Bulletin

Summary

IBM TX Standard is affected by an Out-of-bounds Write vulnerability and by a Use of Inherently Dangerous Function vulnerability due to the way that the product uses certain C library functions. IBM TX Standard has changed the C library functions that it uses in order to address these vulnerabilities.

Vulnerability Details

CVEID: CVE-2025-1330 *(https://www.cve.org/CVERecord?id=CVE-2025-1330)*
DESCRIPTION: IBM CICS TX and IBM TXSeries for Multiplatforms could allow a local user to execute arbitrary code on the system due to failure to handle DNS return requests by the gethostbyname function.
CWE: CWE-787: Out-of-bounds Write *(https://cwe.mitre.org/data/definitions/787.html)*
CVSS Source: IBM
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-2025-1329 *(https://www.cve.org/CVERecord?id=CVE-2025-1329)*
DESCRIPTION: IBM CICS TX and IBM TXSeries for Multiplatforms could allow a local user to execute arbitrary code on the system due to failure to handle DNS return requests by the gethostbyaddr function.
CWE: CWE-787: Out-of-bounds Write *(https://cwe.mitre.org/data/definitions/787.html)*
CVSS Source: IBM
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-2025-1331 *(https://www.cve.org/CVERecord?id=CVE-2025-1331)*
DESCRIPTION: IBM CICS TX and IBM TXSeries for Multiplatforms could allow a local user to execute arbitrary code on the system due to the use of unsafe use of the gets function.
CWE: CWE-242: Use of Inherently Dangerous Function *(https://cwe.mitre.org/data/definitions/242.html)*
CVSS Source: IBM

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)

Affected Products and Versions

Affected Product(s)	Version(s)
IBM CICS TX Standard	11.1

Remediation/Fixes

IBM strongly recommends addressing the vulnerabilities now by downloading and applying the below fix.

Product	Version	Platform	Remediation/Fix
IBM CICS TX Standard	11.1	Linux	Download and apply the fix from Fix Central *(https://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FOther+software%2FCICS+TX+Standard&fixids=ibm-cics-tx-standard-image-11.1.0.0-ifix31&source=SAR)* .

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

08 May 2025: 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:

CICS TX *(https://www.ibm.com/mysupport/s/topic/0TO0z000000Zy60GAC)*

Software version:

11.1

Operating system(s):

Linux

Document number:

7232923

Modified date:

08 May 2025