



Security Bulletin: IBM TX Advanced 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 Advanced 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 Advanced has changed the C library functions that it uses in order to address these vulnerabilities.

Vulnerability Details

CVEID: [CVE-2025-1329](https://www.cve.org/CVERecord?id=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) (<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-2025-1330](https://www.cve.org/CVERecord?id=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) (<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) (<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) (<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 Advanced	10.1
IBM CICS TX Advanced	11.1

Remediation/Fixes

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

Product	Version	Platform	Remediation/Fix
IBM CICS TX Advanced	10.1	Linux	Download and apply the fix from Fix Central (https://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FOther+software%2FCICS+TX+on+Cloud&fixids=ibm-cics-tx-advanced-docker-image-10.1.0.0-ifix38&source=SAR) .
IBM CICS TX Advanced	11.1	Linux	Download and apply the fix from Fix Central (https://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FOther+software%2FCICS+TX+on+Cloud&fixids=ibm-cics-tx-advanced-image-11.1.0.0-ifix30&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

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

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document Information

More support for:

[CICS TX](https://www.ibm.com/mysupport/s/topic/OTO0z000000Zy60GAC) (<https://www.ibm.com/mysupport/s/topic/OTO0z000000Zy60GAC>)

Software version:

10.1, 11.1

Operating system(s):

Linux

Document number:

7232924

Modified date:

08 May 2025