



IBM CICS Transaction Gateway for Multiplatforms Information Disclosure

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-0977 |
| State | PUBLISHED |
| Assigner | ibm |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-16 14:18:07 UTC |
| Updated | 2026-04-02 14:08:57 UTC |
| Description | IBM CICS Transaction Gateway for Multiplatforms 9.3 and 10.1 could allow a user to transfer or view files due to improper e |

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

EPSS: 0.000050000 probability, percentile 0.002070000 (date 2026-04-02)

Problem Types: CWE-284 | NVD-CWE-Other | CWE-284 CWE-284

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 7.1 | HIGH | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N |
| 3.1 | psirt@us.ibm.com | Secondary | 5.1 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N |
| 3.1 | CNA | CVSS | 5.1 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|--------------------------|---------|--------|---------|----------|
| Application | ibm | Cics Transaction Gateway | 10.1 | All | All | All |
| Application | ibm | Cics Transaction Gateway | 9.3 | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------|---|---------------|---------------|
| CNA | IBM | CICS Transaction Gateway For Multiplatforms | affected 9.3 | Not specified |
| CNA | IBM | CICS Transaction Gateway For Multiplatforms | affected 10.1 | Not specified |

References

| Reference | Source | Link | Tags |
|--|------------------|--|---------------------|
| www.ibm.com/support/pages/node/7263518 | psirt@us.ibm.com | www.ibm.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: IBM strongly recommends addressing the vulnerabilities now by configuring proper egress/ingress policies at either the POD or HOST level. More details as to how to do this are described in the following CICS Transaction Gateway for Multiplatforms documentation. ProductVRMFRemediation/First FixCICS Transaction Gateway for Multiplatforms9.3Refer to this documentation <https://www.ibm.com/docs/en/cics-tg-multi/9.3.0> CICS Transaction Gateway for Multiplatforms10.1Refer to this documentation <https://www.ibm.com/docs/en/cics-tg-multi/10.1.0>

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)