



CVE-2021-38934

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-38934
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 21:15:00 UTC
Updated	2022-09-02 18:44:00 UTC
Description	IBM Engineering Test Management 7.0, 7.0.1, and 7.0.2 is vulnerable to cross-site scripting. This vulnerability allows users

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Engineering Test Management	7.0.0	All	All	All
Application	ibm	Engineering Test Management	7.0.1	All	All	All
Application	ibm	Engineering Test Management	7.0.2	All	All	All
Application	ibm	Rational Quality Manager	6.0.6	All	All	All
Application	ibm	Rational Quality Manager	6.0.6.1	All	All	All

References

Reference

- Security Bulletin: Custom "Execution States" names on IBM Engineering Test Management TCER pages are vulnerable to XSS (CVE-2021-3
- IBM X-Force Exchange
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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