



CVE-2017-1739

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

Summary

CVE	CVE-2017-1739
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-11 17:29:00 UTC
Updated	2018-01-31 16:25:00 UTC
Description	IBM Curam Social Program Management 6.0.5, 6.1.1, 6.2.0, and 7.0.1 is vulnerable to cross-site scripting. This vulnerability

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Curam Social Program Management	6.0.5.0	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.1	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.10	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.2	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.3	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.4	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.5	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.6	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.7	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.8	All	All	All
Application	ibm	Curam Social Program Management	6.0.5.9	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.0	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.1	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.2	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.3	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.4	All	All	All
Application	ibm	Curam Social Program Management	6.1.0.5	All	All	All

[illegible]

Application	ibm	Curam Social Program Management	6.1.0.5	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.0	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.1	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.2	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.3	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.4	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.5	All	All	All
Application	ibm	Curam Social Program Management	6.1.1.6	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.0	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.1	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.2	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.3	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.4	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.5	All	All	All
Application	ibm	Curam Social Program Management	6.2.0.6	All	All	All
Application	ibm	Curam Social Program Management	7.0.0.0	All	All	All
Application	ibm	Curam Social Program Management	7.0.0.1	All	All	All
Application	ibm	Curam Social Program Management	7.0.0.2	All	All	All
Application	ibm	Curam Social Program Management	7.0.1.0	All	All	All
Application	ibm	Curam Social Program Management	7.0.1.1	All	All	All

References

Reference

IBM Cúram Social Program Management CVE-2017-1739 Cross Site Scripting Vulnerability

IBM X-Force Exchange

Security Bulletin: Fix available for Stored Cross Site Scripting (XSS) Vulnerability in IBM Cúram Social Program Management (CVE-2017-1739)

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.

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