



CVE-2017-1683

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

Summary

CVE	CVE-2017-1683
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-11 21:29:00 UTC
Updated	2017-12-26 15:40:00 UTC
Description	IBM Connections Engagement Center 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary HTML and JavaScript into the page. An attacker can use this vulnerability to steal sensitive information, such as cookies and session IDs, and to perform other malicious actions.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Connections Engagement Center	6.0	All	All	All
Application	ibm	Connections Engagement Center	6.0	All	All	All

References

Reference	Source	Link
IBM Connections Engagement Center Cross Site Scripting and Information Disclosure Vulnerabilities	BID	www.securityfocus.com
IBM notice: The page you requested cannot be displayed	CONFIRM	www.ibm.com
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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