



CVE-2017-1713

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

Summary

CVE	CVE-2017-1713
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 15:59:00 UTC
Updated	2019-10-09 23:26:00 UTC
Description	IBM InfoSphere Streams 4.2.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Infosphere Streams	4.2.1	All	All	All
Application	ibm	Infosphere Streams	4.2.1	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	VDB Entry, Vendor Acknowledgment
Security Bulletin: There is a weak ciphers vulnerability in IBM Streams	CONFIRM	www.ibm.com	Patch, 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.

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

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