CVE-2017-1664

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-1664
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-04 17:29:00 UTC
Updated	2018-01-12 20:09:00 UTC
Description	IBM Tivoli Key Lifecycle Manager 2.5, 2.6, and 2.7 uses weaker than expected cryptographic algorithms that could allow an

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Security Key Lifecycle Manager	2.5.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.2	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.3	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.4	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.5	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.6	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.7	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.8	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.2	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.3	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0.2	All	All	All

Application	Ibm	Security Key Lifecycle Manager	2.5.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.2	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.3	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.4	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.5	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.6	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.7	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.5.0.8	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.2	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.6.0.3	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0.1	All	All	All
Application	Ibm	Security Key Lifecycle Manager	2.7.0.2	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	MISC	exchang
Security Bulletin: IBM Security Key Lifecycle Manager uses broken or risky cryptographic algorithm (CVE-2017-1664)	CONFIRM	www.ibn
IBM Security Key Lifecycle Manager CVE-2017-1664 Information Disclosure Vulnerability	BID	www.sec
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**