



CVE-2018-1388

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

Summary

CVE	CVE-2018-1388
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-07 17:29:00 UTC
Updated	2018-12-20 11:29:00 UTC
Description	GSKit V7 may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding. IBM X-Force

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	IBM	Websphere Mq	7.0.1.0	All	All	All
Application	IBM	Websphere Mq	7.0.1.1	All	All	All
Application	IBM	Websphere Mq	7.0.1.10	All	All	All
Application	IBM	Websphere Mq	7.0.1.11	All	All	All
Application	IBM	Websphere Mq	7.0.1.12	All	All	All
Application	IBM	Websphere Mq	7.0.1.13	All	All	All
Application	IBM	Websphere Mq	7.0.1.14	All	All	All
Application	IBM	Websphere Mq	7.0.1.2	All	All	All
Application	IBM	Websphere Mq	7.0.1.3	All	All	All
Application	IBM	Websphere Mq	7.0.1.4	All	All	All
Application	IBM	Websphere Mq	7.0.1.5	All	All	All
Application	IBM	Websphere Mq	7.0.1.6	All	All	All
Application	IBM	Websphere Mq	7.0.1.7	All	All	All
Application	IBM	Websphere Mq	7.0.1.8	All	All	All
Application	IBM	Websphere Mq	7.0.1.9	All	All	All
Application	IBM	Websphere Mq	7.0.1.0	All	All	All
Application	IBM	Websphere Mq	7.0.1.1	All	All	All

Application	Ibm	Websphere Mq	7.0.1.10	All	All	All
Application	Ibm	Websphere Mq	7.0.1.11	All	All	All
Application	Ibm	Websphere Mq	7.0.1.12	All	All	All
Application	Ibm	Websphere Mq	7.0.1.13	All	All	All
Application	Ibm	Websphere Mq	7.0.1.14	All	All	All
Application	Ibm	Websphere Mq	7.0.1.2	All	All	All
Application	Ibm	Websphere Mq	7.0.1.3	All	All	All
Application	Ibm	Websphere Mq	7.0.1.4	All	All	All
Application	Ibm	Websphere Mq	7.0.1.5	All	All	All
Application	Ibm	Websphere Mq	7.0.1.6	All	All	All
Application	Ibm	Websphere Mq	7.0.1.7	All	All	All
Application	Ibm	Websphere Mq	7.0.1.8	All	All	All
Application	Ibm	Websphere Mq	7.0.1.9	All	All	All

References

Reference

IBM Global Security Kit CVE-2018-1388 Information Disclosure Vulnerability

Security Bulletin: WebSphere MQ is vulnerable to disclosing side channel information via discrepancies between valid and invalid PKCS#1 padding

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.