



CVE-2018-1648

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

Summary

CVE	CVE-2018-1648
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-05 17:29:00 UTC
Updated	2018-12-26 16:39:00 UTC
Description	IBM QRadar SIEM 7.2 and 7.3 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	Qradar Incident Forensics	All	All	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	-	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p1	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p10	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p11	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p12	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p13	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p3	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p4	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p5	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p6	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p7	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p8	All	All
Application	ibm	Qradar Incident Forensics	7.2.8	p9	All	All
Application	ibm	Qradar Incident Forensics	7.3.1	-	All	All
Application	ibm	Qradar Incident Forensics	7.3.1	p1	All	All
Application	ibm	Qradar Incident Forensics	7.3.1	p2	All	All

Application	lbn	Qradar Incident Forensics	7.3.1	p3	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p4	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p5	All	All
Application	lbn	Qradar Incident Forensics	All	All	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	-	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p1	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p10	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p11	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p12	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p13	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p3	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p4	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p5	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p6	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p7	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p8	All	All
Application	lbn	Qradar Incident Forensics	7.2.8	p9	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	-	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p1	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p2	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p3	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p4	All	All
Application	lbn	Qradar Incident Forensics	7.3.1	p5	All	All

References						
Reference	Source	Link		Tags		
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com		VDB Entry, Vendor Advisory		
Security Bulletin:	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)