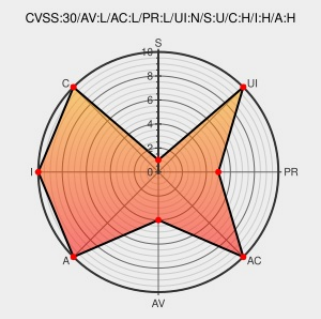
CVE-2016-2871

Published on: 11/30/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2871

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Qradar Security Information And Event Manager from Ibm contain the following vulnerability:

IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 uses cleartext storage for unspecified passwords, which allows local users to obtain sensitive information by reading a configuration file.

CVE-2016-2871 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IBM Security Bulletin: IBM QRadar SIEM is vulnerable to clear text passwords. (CVE-2016-2871) - United States	Patch, Vendor Advisory, www-01.ibm.com, text/html	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21987769

IBM QRadar Security Information and Event Manager Local Information Disclosure Vulnerability

cve.report (archive) text/html

BID 94861

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Qradar Security Information And Event Manager	7.2.0	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.1	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.2	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.3	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.4	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.5	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.6	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.0	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.1	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.2	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.3	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.4	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.5	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.2.6	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	All	mr1	All	All

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.2:*:*:*:*:*:*:*

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.3:*:*:*:*:*:*:*

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.4:*:*:*:*:*:*:*

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.5:*:*:*:*:*:*:*

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.2.6:*:*:*:*:*:*:*

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:*:mr1:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→