CVE-2016-2873

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

Summary

CVE	CVE-2016-2873
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-30 18:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	SQL injection vulnerability in IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 allows remote authenticated

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.005740000 probability, percentile 0.688610000 (date 2026-05-08)

Problem Types: CWE-89 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

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	All	mr1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
IBM Security Bulletin: IBM QRadar SIEM is vulnerable to SQL Injection. (CVE-2016-2873) - United States	af854a3a-2127-422b-91ae-364da
IBM QRadar Security Information and Event Manager CVE-2016-2873 SQL Injection Vulnerability	af854a3a-2127-422b-91ae-364da

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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