



CVE-2023-22875

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

Summary

CVE	CVE-2023-22875
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 19:15:00 UTC
Updated	2023-11-07 04:07:00 UTC
Description	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed h

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Qradar Security Information And Event Manager	7.4.0	-	All	All
Application	ibm	Qradar Security Information And Event Manager	7.5.0	-	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com
Security Bulletin: IBM QRadar SIEM is vulnerable to possible information disclosure [CVE-2023-22875]	MISC	www.ibm.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378490 IBM QRadar SIEM Information Disclosure Vulnerability (6855643)

© [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](#)