

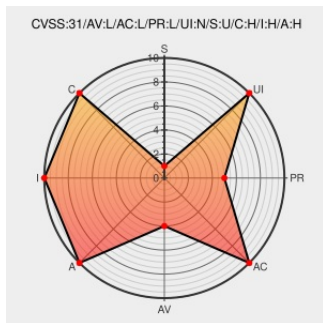


CVE-2020-4270

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 06/29/2022 09:19:00 PM UTC

CVE-2020-4270

[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 7.3.0 to 7.3.3 Patch 2 could allow a local user to gain escalated privileges due to weak file permissions. IBM X-ForceID: 175846.

CVE-2020-4270 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **Qradar** version **7.3.3.Patch2**

Affected Vendor/Software: [IBM](#) - **QRadar** version **7.3.0**

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
-------------	------	------

QRadar Community Edition 7.3.1.6 Insecure File Permissions ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/157335/QRadar-Community-Edition-7.3.1.6-Insecure-File-Permissions.html
Full Disclosure: Local privilege escalation in QRadar due to run-result-reader.sh insecure file permissions	seclists.org text/html	 FULLDISC 20200421 Local privilege escalation in QRadar due to run-result-reader.sh insecure file permissions
Security Bulletin: IBM QRadar SIEM is vulnerable to privilege escalation (CVE-2020-4270)	Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6189657
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-qradar-cve20204270-priv-escalation (175846)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	All	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	-	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	p1	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	p2	All	All
Application	Ibm	Qradar Security Information And Event Manager	All	All	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	-	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	p1	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	p2	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:-:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p1:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p2:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:*****:						
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:-:*****:						

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p1:*****:
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:p2:*****:
cpe:2.3:o:linux:linux_kernel:-:*****:
cpe:2.3:o:linux:linux_kernel:-:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? IBM QRadar 7.3.0 to 7.3.3 Patch 2 could ... CVE-2020-4270 Link for more: alerts.remotelyrmm.com/CVE-2020-4270	2022-06-29 22:30:53
← Previous ID		Next ID →

© CVE.report 2023   | 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)