

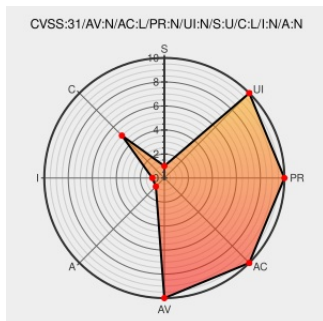


CVE-2021-38939

Published on: Not Yet Published

Last Modified on: 05/04/2022 02:55:00 PM UTC

CVE-2021-38939

[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 7.3, 7.4, and 7.5 stores potentially sensitive information in log files that could be read by an user with access to creating domains. IBM X-Force ID: 211037.

CVE-2021-38939 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.3.3**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.4.3**

Affected Vendor/Software: [IBM](#) - **QRadar SIEM** version **7.5.0**

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Security Bulletin: IBM QRadar SIEM is vulnerable to using components with Known Vulnerabilities	www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6574787
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ibm-qradar-cve202138939-info-disc (211037)

By selecting these links, you may be leaving CVEreport workspace. 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	fix_pack_1	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_2	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_3	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_4	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_5	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_6	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_7	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_8	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.3.3	fix_pack_9	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.3	-	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.3	fix_pack_1	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.3	fix_pack_2	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.3	fix_pack_3	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.5.0	-	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:gradar security information and event manager:7.3.3::*:.*:.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:ibm:gradar security information and event manager:7.3.3:fix pack 1:::*.*.*.*.*

cpe:2.3:a:ibm:gradar security information and event manager:7.3.3:fix pack 2:::*:*:*:*:

cpe:2.3:a:ibm:gradar_security_information_and_event_manager:7.3.3:fix_pack_3:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_4:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_5:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_6:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_7:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_8:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_9:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.3:-:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.3:fix_pack_1:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.3:fix_pack_2:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.3:fix_pack_3:~::~~::~~::~~::~~::
cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.5.0:-:~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:-:~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-38939 : #IBM QRadar SIEM 7.3, 7.4, and 7.5 stores potentially sensitive information in log files that coul... twitter.com/i/web/status/1...	2022-04-27 15:30:23
 /r/netcve	CVE-2021-38939	2022-04-27 16:39:20

[← 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](#)