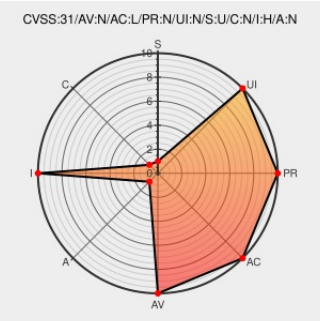
CVE-2021-38878

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2021-38878

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, 7.4, and 7.5 could allow a malicious actor to impersonate an actor due to key exchange without entity authentication. IBM X-Force ID: 208756.

CVE-2021-38878 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as HIGH 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: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve202138878-sec-bypass (208756)
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

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	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:qradar_security_information_and_event_manager:7.3.3:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_1:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.3.3:fix_pack_2:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_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-2021-38878 : #IBM QRadar 7.3, 7.4, and 7.5 could allow a malicious actor to impersonate an actor due to key exc… twitter.com/i/web/status/1…	2022-04-27 15:29:46
/r/netcve	CVE-2021-38878	2022-04-27 16:39:18

© 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 registred 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