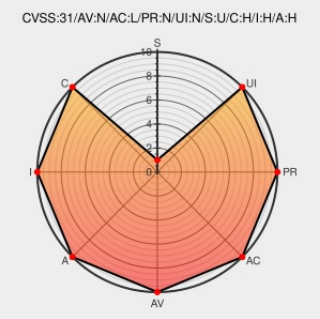
CVE-2020-4979

Published on: 05/05/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

CVE-2020-4979

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 and 7.4 is vulnerable to insecure inter-deployment communication. An attacker that is able to comprimise or spoof traffic between hosts may be able to execute arbitrary commands. IBM X-Force D: 192538.

CVE-2020-4979 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **IBM** - **QRadar SIEM** version **7.3**

Affected Vendor/Software: **IBM** - **QRadar SIEM** version **7.4**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-qradar-cve2020497 9-code-exec (192538)
Security Bulletin: IBM QRadar SIEM is vulnerable to insecure inter-deployment communication (CVE-2020-4979)	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6449668

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2020-4979

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	7.4.2	-	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.2	fix_pack_1	All	All
Application	Ibm	Qradar Security Information And Event Manager	7.4.2	fix_pack_2	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:7.4.2:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.2:fix_pack_1:*:*:*:*:*:*:

cpe:2.3:a:ibm:qradar_security_information_and_event_manager:7.4.2:fix_pack_2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-4979 : #IBM QRadar SIEM 7.3 and 7.4 is vulnerable to insecure inter-deployment communication. An attacker… twitter.com/i/web/status/1…	2021-05-05 15:48:59
/r/netcve	CVE-2020-4979	2021-05-05 16:41:52

← Previous ID

Next ID→